XT-Family

Encrypted Ethernet Tunnel

User's Guide

Revised March 14, 2025

Firmware Version 1.x

Certifications

FCC Statement

This device complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules.

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

RoHS

Some models of this product is available in RoHS versions.

This product is available in RoHS versions.

Table of Contents

Chapter 1
Introduction

This chapter provides an overview of the EtherSeries XT Encrypted Ethernet Tunnel Bridge's features and capabilities.

Congratulations on the purchase of your new EtherSeries Encrypted Ethernet Bridge. This is a simple, easily configured tunneling device containing multiple ethernet interfaces. Some models also have serial interfaces.

Two or more bridges connect using either TCP/IP or UDP/IP using any insecure IP connection path, via any IP WAN media such as digital radios, satellite, DSL, or cable modems. They tunnel all Ethernet packets from the secure interface of each XT device to the secure interface of other XT devices. The XT products are compatible with other DCB products in the UT, ET, and XT line. A software client is also available for Windows workstations.

The bridge transports all valid Ethernet protocols. It provides a virtual private network by bridging the two LANs with an IP tunnel that may be encrypted using the AES algorithm. AES is available in 128, 192, or 256 bit versions. Filtering is available based upon many packet characteristics including IP or MAC addresses, ports, and Protocol types. Multicast, Unicast, and 802.1Q VLAN tagging is supported.

When used in its simplest mode, two bridges might "extend" a secure LAN segment to another physical location via an insecure path. They may be used behind firewalls and NAT routers to "extend" a flat subnet across other IP address range networks such as the Internet.

Note that configuration screen examples shown in this manual are for the XT family products which have differing options. Some display screen options may differ slightly from what your unit displays.

EtherSeries XT-Family Applications

The XT Family products connect multiple LAN segments by using TCP or UDP IP protocols between the bridges. It is commonly used to connect a remote LAN to a central LAN using an insecure path. In this installation, the bridges connect using IP, authenticate each other, negotiate an encrypted link, and then bridge all allowed traffic between the two LANs.

The encrypted ethernet bridge is also used to connect a single location to multiple remote sites. In this application, remote sites may be "daisy-chained" to allow multiple locations to communicate via insecure links.

The bridge is normally configured to auto-connect upon power-up. They are used in client-server combinations. In this mode, the client unit will connect to a remote bridge through any valid IP path, and may be configured to use DHCP. Any unit may be configured as a client, a server, or both simultaneously.

The client units may be configured to obtain an external IP address via DHCP. If configured in this manner, they may be used in a "plug-and-play" mode for mobile or portable applications. Simply plug it into an ethernet port at any location offering a dynamic DHCP IP address, and it will self-configure and connect to the bridge at the home location… providing a virtual private network between the locations.

Other Features

Other Protocols

The bridge uses either the UDP/IP or TCP/IP protocol to connect to its remote peers. It does pass all ethernet packets such as IP, IPX, AppleTalk, and other non-routable protocols through the encrypted IP tunnel. It handles Multi-cast IP including IGMP Report Proxy features. An XT unit will connect with ET, UT, and XP peers using either or both TCP and UDP protocols. While it uses UDP or IP between the XT units, they bridge all ethernet protocols.

DHCP Protocol

The bridge supports the DHCP protocol as a client or server. DHCP may be served through the tunneled link. In server mode, Dynamic DNS services are available.

Extensive Filtering

The bridge supports extensive filtering based upon IP addresses, MAC addresses, or Protocol type. Filtering may be configured as “shall pass” or “shall deny” defaults with configured exceptions.

802.1q VLAN

The bridge passes 802.1Q VLAN tagged packets.

Upgradeable Firmware

Firmware upgrades may be installed using any web browser. Upgrade may accomplished remotely through a working bridge.

Security and Firewall Features

The bridge supports a number of security features. On the “insecure” side, all traffic is encrypted, including the XT to XT negotiation. The encryption methodology is industry-standard AES. Once configured, only workstations on the “secure” side of a unit may be used to configure or control it. When in UDP mode, the insecure side interface appears to be a “black hole” to port scanners.

On-board Tools

The bridge contains diagnostic tools such as extensive logging, traceroute, ping, bandwidth test, and a simple packet sniffer to aid in network troubleshooting.

Simple Web Proxy

A simple light weight web proxy is included. This operation allows web traffic from the trusted interface to be passed to the untrusted interface, while all other traffic is tunneled to the other bridge. **This is not a full featured web proxy, but is available for special cases where configuration of network equipment from the inside is needed.**

Single-Interface operation

Normally, the XT bridge is a “lump in the cord” between the secure network and the external networks. The XT-Family bridge may also be configured in a "single-interface" appliance mode. See details in the manual and applications note.

Package Contents

You should find the following items packaged with your EtherSeries Bridge:

- The XT Bridge
- Power Cable
- This User’s Guide CDROM

If any of the above are missing, contact your dealer immediately.

Software Requirements

The bridge supports IP and associated protocols such as UDP, ICMP, DHCP, multi-cast, and any protocol built upon IP or TCP/IP**. It also bridges any valid Ethernet protocol**. If your model includes a serial interface, the initial IP address may be entered using any terminal or terminal emulation software on a PC, or the default may be used if appropriate for your network.

Any standard web browser may be used for configuration once the bridge is configured with a valid IP address.

The XT-Family of bridges will link with other XT-Family bridges, UT-Family, and ET-Family bridges as well as the UT-Soft software client.

XT-3303

Introduction

The XT-3303 model bridge contains three Ethernet ports and one serial port. All of the Ethernet ports are "soft". Out of the box, the port to the far left is the LAN2 untrusted port and the remaining two ports are LAN1 trusted ports. However, the user is free to reconfigure each physical port to belong to LAN1, LAN2, or LAN3. This unit has a LAN3 that may be used as a second untrusted interface.

This model supports passive POE-IN on eth0. The ports are all 10/100/1000. Typical throughput is 20 Mbps with uni-directional AES-256.

Configuration

This model contains a serial interface that may be used for initial setup (if needed). If the default IP address (192.168.0.1) is not appropriate for your LAN, you may connect a terminal to the serial port. Follow the command line setup instructions to configure a compatible IP address. Once a compatible IP address is available, the browser setup screens are required for additional configuration. The serial port is configured to operate in setup mode by default. However, if the port does not appear to work, it may be that the serial port has been disabled or configured for a different mode.

To reset to defaults, power up the device. Wait a minimum of 1 minute. Press and hold the reset button for 5 or more seconds. Release the button. This action erases the configuration and reboots the unit to defaults.

XT-3303

LED Indicators

Each LAN connector has two LEDs. The green LED indicates link and will blink with activity. The yellow LED is only enabled in eth0 and will illuminate in 10/100Mb mode. It is off in 1000Mb mode.

There are two status LEDs between the power connector and eth0. The lower, blue LED, indicates power. The upper, green LED, indicates boot status. It will blink several times during boot, but will remain off once the system is fully running.

Ethernet Connectors

The 10/100/1000BaseT connectors are auto-sensing. Eth0 supports passive POE-IN. Please note this is NOT the same as 802.3af POE. The unit cannot be powered using an 802.3af POE switch.

RS-232 Panel Connector

The DE-9 (PC 9-pin) connector is used for initial IP addressing setup and a TCP/UDP terminal server connection. **A cross-over cable is required to use this with any standard PC serial port.** Terminal configuration is 9600 bps, 8N1.

XT-3305

Introduction

The XT-3305 model bridge contains five Ethernet ports. All of the Ethernet ports are "soft". Out of the box, the port to the far left is the LAN2 untrusted port and the remaining ports are LAN1 trusted ports. However, the user is free to reconfigure each physical port to be a LAN1, LAN2, or LAN3 port. This unit has a LAN3 that may be used as a second untrusted interface.

This model supports POE-IN on eth0, and POE-OUT on eth4. The ports are all 10/100/1000.
Each physical port may be configured as one of three LAN ports. One of those (LAN1) is trusted, and two (LAN2 and LAN3) are untrusted. Typical throughput is 20 Mbps with uni-directional AES-256.

Configuration

The default IP address is 192.168.0.1. For initial configuration, temporarily configure a web browser workstation to a compatible local address. Once a compatible IP address is available, the browser setup screens are required for additional configuration.

To reset to defaults, power up the device. Wait a minimum of 1 minute. Press and hold the reset button for 5 or more seconds. Release the button. This action erases the configuration and reboots the unit to defaults.

XT-3305

Top Panel LED Indicators

LAN LEDs are in the top of the enclosure. They are ON with link and blink with activity.

There is a power LED also in the top of the enclosure.

Ethernet Connectors

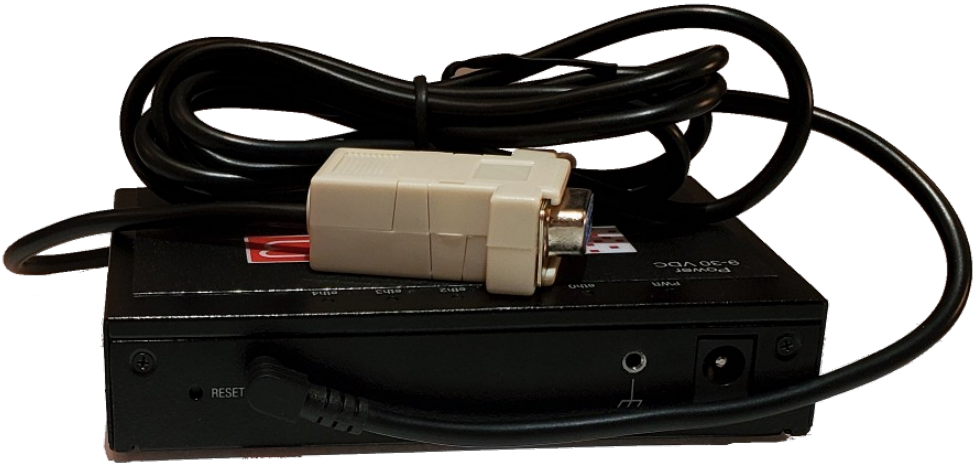
The 10/100/1000BaseT connectors are auto-sensing. Eth0 can be configured for passive POE-IN. Eth4 may be configured for passive POE-OUT. Please note that passive POE is not the same as 802.3af POE. This unit cannot be powered from an 802.3af POE switch nor can it power an 802.3af POE device.

XT-3305s

Introduction

The XT-3305s is a variation of the XT-3305 described above and shares the same characteristics. In addition, it supports one RS-232 serial port.

XT-3305s Rear



RS-232 Serial Port

The RS-232 serial port is located on the rear of the enclosure and is implemented using a 2.5mm TRS jack (mini-audio jack). The interface supports Rx, Tx, and Ground. Cables terminated with a male DE-9 and female DE-9 are available from DCB. The serial port may be used for initial configuration and also to support TCP and UDP terminal server functions.

XT-hEX

Introduction

The XT-hEX model bridge contains five Ethernet ports. All of the Ethernet ports are "soft". Out of the box, the port to the far left is the LAN2 untrusted port and the remaining ports are LAN1 trusted ports. However, the user is free to reconfigure each physical port to be a LAN1, LAN2, or LAN3 port. This unit has a LAN3 that may be used as a second untrusted interface.

This model supports passive POE-IN on eth1 port. The ports are all 10/100/1000.
Each physical port may be configured as one of three LAN ports. One of those (LAN1) is trusted, and two (LAN2 and LAN3) are untrusted. Typical throughput is 20 Mbps with uni-directional AES-256.

Note: This unit is functionally similar to the XT-3305. It differs in that it does not support passive POE output on any of the Ethernet ports. It is slightly larger in size and utilizes a plastic enclosure.

Configuration

The default IP address is 192.168.0.1. For initial configuration, temporarily configure a web browser workstation to a compatible local address. Once a compatible IP address is available, the browser setup screens are required for additional configuration.

To reset to defaults, power up the device. Wait a minimum of 1 minute. Press and hold the reset button for 5 or more seconds. Release the button. This action erases the configuration and reboots the unit to defaults.

XT-hEX

LED Indicators

LAN LEDs are in the top of the enclosure. They are ON with link and blink with activity.

There are two status LEDs located on the front. The blue LED, indicates power. The green LED, indicates boot status. It will blink several times during boot, but will remain off once the system is fully running.

Ethernet Connectors

The 10/100/1000BaseT connectors are auto-sensing. Eth1 can be configured for passive POE-IN. Please note that passive POE is not the same as 802.3af POE. This unit cannot be powered from an 802.3af POEswitch.

XT-3306

Introduction

The XT-3306 model bridge contains one untrusted ethernet port, a trusted ethernet port with four port ethernet switch supporting VLAN tagging, and one serial port. It is designed for operation with a direct wired ethernet WAN connection using a public network, DSL modem, cellular broadband, WIFI, satellite, Cable modem, or any network path terminating in copper ethernet. It supports up to 8 simultaneous remote XT, ET, or UT units when in server mode. Typical throughput is 15 Mbps.

Configuration

This model contains a serial interface that may be used for initial setup (if needed), as a TCP port server, or UDP port server. If the default IP address (192.168.0.1) is not appropriate for your LAN, connect a terminal to the serial port following the instructions in the configuration section. If enabled, the setup port is always active on this model**.** Follow the command line setup instructions to configure a compatible IP address. Once a compatible IP address is available, the browser setup screens are required for additional configuration.

XT-3306

Reset To Factory Defaults

If you know the IP address, you may browse to the Administration screen – Set All Defaults. If the IP address is unknown, use the serial connection setup method (Chapter 2), and answer Yes when asked if you wish to reset the unit to factory defaults. The factory default IP address for the trusted side Ethernet port (LAN1) is 192.168.0.1. Another method uses the hardware setup switch:

The unit can be set to temporarily set to defaults by pressing and holding the setup switch during power-up. The sequence is:

1) Apply power, blue (bottom) led will go on then the green (top) led will go on.
2) Wait for the green led to go off.
3) Press and hold the setup switch.
4) Wait for the green led to blink on then off.
5) The switch may be released.
6) The serial port will be in setup mode and the unit can be accesses from the default address.

Note) The default settings are not written to NV memory. The user must store the settings from either the serial port or the web interface.

Rear Panel LED Indicators

One set of indicators For Each Ethernet Port

- The green LED to the left of each ethernet port is the Ethernet Status indicator. It is lit when the port is connected to a 1000BaseT switch. It is not lit for 10BaseT and 100Baset connections.

- The yellow LED to the right of each ethernet port is a LAN activity indicator. This LED flashes with activity on the Ethernet (even if the activity isn't directly to this unit).

Side Panel LED Indicators

- Lower Blue LED is a power indicator. It should be on.
- Upper LED is not used

RS-232 Panel Connector

The DE-9 (PC 9-pin) connector is used for initial IP addressing setup and a TCP/UDP terminal server connection. **A cross-over cable is required to use this with any standard PC serial port.** Terminal configuration is 9600 bps, 8N1 .

Ethernet Connectors

The 10/100/1000BaseT connectors are auto-sensing. The Untrusted port will power the unit from a POE switch or power injector. The built-in switch is does not supply POE power to downstream devices.

XT-6606

Introduction

The XT-6606 model bridge contains two untrusted ethernet ports, one trusted ethernet port supporting VLAN tagging, and one serial port. It is designed for operation with a direct wired ethernet WAN connection using a public network, DSL modem, cellular broadband, WIFI, satellite, Cable modem, or any network path terminating in copper ethernet. It supports up to fifty simultaneous remote XT, UT, or ET units when in server mode. Typical throughput is 63 Mbps.

Configuration

This model contains a serial interface that may be used for initial setup (if needed), as a TCP port server, or UDP port server. If the default IP address (192.168.0.1) is not appropriate for your LAN, connect a terminal to the serial port following the instructions in the configuration section. If enabled, the setup port is always active on this model**.** Follow the command line setup instructions to configure a compatible IP address. Once a compatible IP address is available, the browser setup screens are required for additional configuration.

XT-6606

Reset To Factory Defaults

If you know the IP address, you may browse to the Administration screen – Set All Defaults. If the IP address is unknown, use the serial connection setup method (Chapter 2), and answer Yes when asked if you wish to reset the unit to factory defaults. The factory default IP address for the trusted side Ethernet port (LAN1) is 192.168.0.1. Another method uses the hardware setup switch:

The unit can be set to temporarily set to defaults by pressing and holding the setup switch during power-up. The sequence is:

1) Apply power, all three green led on the front will illuminate.
2) Wait for the green leds 2 and 3 to go off.
3) Press and hold the setup switch (located behind the small hole in the front panel).
4) Wait for the green led 2 to blink on then off (approximately 15 seconds later).
5) The switch may be released.
6) The serial port will be in setup mode and the unit can be accesses from the default address

Note) The default settings are not written to NV memory. The user must store the settings from either the serial port or the web interface.

Rear Panel LED Indicators

One set of indicators For Each Ethernet Port

- The green LED to the left of each ethernet port is a LAN activity indicator. This LED flashes with activity on the Ethernet (even if the activity isn't directly to this unit).
- The yellow/green LED to the right of each ethernet port is the Ethernet Status indicator. It is lit amber when the port is connected to a 1000BaseT switch, green for 100BaseT. It is not lit for 10BaseT connections.

Front Panel LED Indicators

- Power indicator. It should be on.

RS-232 Panel Connector

The DE-9 (PC 9-pin) connector is used for initial IP addressing setup and a TDP/UDP terminal server connection. **A cross-over cable is required to use this with any standard PC serial port.** Terminal configuration is 9600 bps, 8N1 .

Ethernet Connectors

The 10/100/1000BaseT connectors are auto-sensing.

USB Connectors

There are two USB connectors. They are interchangeable, and only the first one that senses a USB device connection is activated. The USB interface is used to transfer security certificates (if used).

XT-6615

Introduction

The XT-6615 model bridge contains four Ethernet ports and one serial ports. It is designed for operation with a direct wired Ethernet WAN connection using a public network, DSL modem, cellular broadband, WIFI, satellite, Cable modem, or any network path terminating in copper Ethernet. It supports up to 50 simultaneous remote XT units.

Configuration

All configuration is performed through the LAN1 interface using a secure web browser. The default LAN1 IP address is 192.168.0.1. Ensure that your PC is configured with a compatible IP address. Using a web browser, enter the URL *https://192.168.0.1* to access the device. This model contains a serial interface that may be used to modify the LAN IP addresses or to reset the device to the factory default configuration. It also supports a HDMI monitor and USB keyboard that can be used for the same purpose.

XT-6615

LED Indicators

Each LAN port has link and activity indicators. The device also has power and SSD activity indicators.

USB Connectors

There are two USB connectors. A USB keyboard and HDMI monitor may be used for initial configuration. Either USB connector may be used

HDMI Connectors

There are two HDMI connectors. A USB keyboard and HDMI monitor may be used for initial configuration. Either HDMI connector may be used.

Audio Connector

The device has an audio connector that is unused for this application.

RS-232 COM Port

The device supports a RS-232 COM port implemented on a RJ45 connector. A cable is supplied with the device that allows the port to be directly connected a standard PC DE9 COM port. The COM port may be used for initial configuration or may be configured to support a terminal server feature. The default COM port configuration is *setup mode, 9600 bps, 8N1*.

Ethernet Connectors

The four 10/100/1000BaseT connectors are auto-sensing. Only LAN1 may be used for initial configuration via a web browser.

XT-6632

Introduction

The XT-6632 model bridge contains two Ethernet ports and two serial ports. It is designed for operation with a direct wired ethernet WAN connection using a public network, DSL modem, cellular broadband, WIFI, satellite, Cable modem, or any network path terminating in copper ethernet. It supports up to 128 simultaneous remote XT units.

Configuration

This model contains a serial interface to be used in initial setup (if needed), as TCP port servers, or UDP port servers. If the default IP address is not appropriate for your LAN, connect a terminal to the serial port following the instructions in the configuration section. If enabled, the setup port is always active on this model**.** Follow the command line setup instructions to configure a compatible IP address. Once a compatible IP address is available, the browser setup screens are much easier to use.

XT-6632 Front

LED Indicators

The front panel LED indicators include an over-temperature warning, LAN Activity, LAN status (two per interface), and power indicator.

USB Connectors

There are two USB connectors. They are interchangeable, and only the first one that senses a USB device connection is activated. The USB interface is used to transfer security certificates (if used).

RS-232 Connectors

The DE-9 (PC 9-pin) connectors are used for command line setup or terminal server ports. A cross-over cable is required to use this with any standard PC serial port. Terminal configuration is 9600 bps, 8N1.

Ethernet Connectors

The two 10/100/1000BaseT connectors are auto-sensing.

Monitor Interface

The unit has an active VGA interface. This interface along with a USB keyboard may be used for initial configuration. Note: an older revision of the hardware had a DVI interface instead of the VGA interface.

Chapter 2
Installation

This Chapter details the installation process for the XT EtherSeries Bridge.

Overview

The bridge is normally configured using a web browser directed to its address. If the default address of 192.168.0.1 is appropriate for your local network, then plug it in and simply direct your web browser to the bridge (using https without using a proxy) and continue with configuration. If this address is not appropriate for your network, the bridge's IP address must be configured using the initial terminal method below if it contains a serial port. If your model does not include a serial port, the configuration workstation must be configured with an appropriate IP address for initial configuration.

The CDROM contains a Configuration Worksheet document and more detailed step-by-step instructions for several commonly used configurations. Printing that document and using it is highly recommended, and will save time when first configuring the bridges.

Quick Start

Quick start instructions are in the following section. Installation is an easy process, but you must have a thorough understanding of IP networking, subnetting, and routing. You should have a network diagram illustrating IP addresses, subnetting, and all IP routing that you intend to use prior to installing the bridge.

Help Screens and Field Edits

The field names on all configuration screens are hyperlinks to context sensitive help screens. Simply click on the field name to bring up a second window with the help information. Close that window to return to your entry screen.

Entries are always tested for valid values. However, there are many "valid" values that are not appropriate for any given configuration. So, "appropriateness" isn't tested. For example, an IP address of 300.400.500.256 will not be accepted, but the field will accept an IP address that is not appropriate for *your* installation.

Installation and Configuration

1. Configure the Bridge's IP address

If the bridge's default address (192.168.0.1) is appropriate for your network or your model does not include a serial interface, skip to step 2, "Connect the Ethernet Cable".

1. Connect a terminal or PC running terminal emulation program (Hyperterm, Procomm, etc) to the serial port of the bridge.
2. Start the terminal emulation program using 9600 bps, 8-bits, No parity, No flow control.
3. Power up the bridge.
4. The Bridge will start up pausing at a configuration screen.

Welcome to Setup. This setup will establish the XT-6632 in

a known state so that you can configure it via a Web Browser.
It will allow you to configure the Ethernet IP address
subnet mask, and gateway. You also have the option to set all
parameters to default, which is the only method to remove
security parameters.

HTTPS port: 443
LAN1 Configuration
IP: 192.168.0.1
SM: 255.255.255.0
GW:
LAN2 Configuration: automatic-via DHCP

Should LAN1 use DHCP to get an IP address (y/[n])?
LAN1 IP Address is currently: 192.168.0.1
Enter new IP Address, or blank for no change:
LAN1 Subnet Mask is currently: 255.255.255.0
Enter new Subnet Mask, or blank for no change:
LAN1 Gateway Address is currently:
Enter new Gateway Address, or blank for no change:

Will LAN1 be connected to an 802.1Q tagged VLAN trunk(y/[n])?

Should LAN2 use DHCP to get an IP address (y/[n])?
LAN2 IP Address is currently: 192.168.2.1
Enter new IP Address, or blank for no change

LAN2 Subnet Mask is currently: 255.255.255.0
Enter new Subnet Mask, or blank for no change:
LAN2 Gateway Address is currently:
Enter new Gateway Address, or blank for no change:

Saving Configuration. Do not cycle power...
Setup complete.

After rebooting the system, you will be able to configure
the unit from a Web Browser. Use the URL https://192.168.0.1
rebooting system.

Login Screen

5. On this screen, you will be asked if you wish to set initial parameters for the interfaces.

6. The bridge will now compress these values and save the configuration to flash memory. Do not cycle power during this time or the unit may be rendered inoperable.

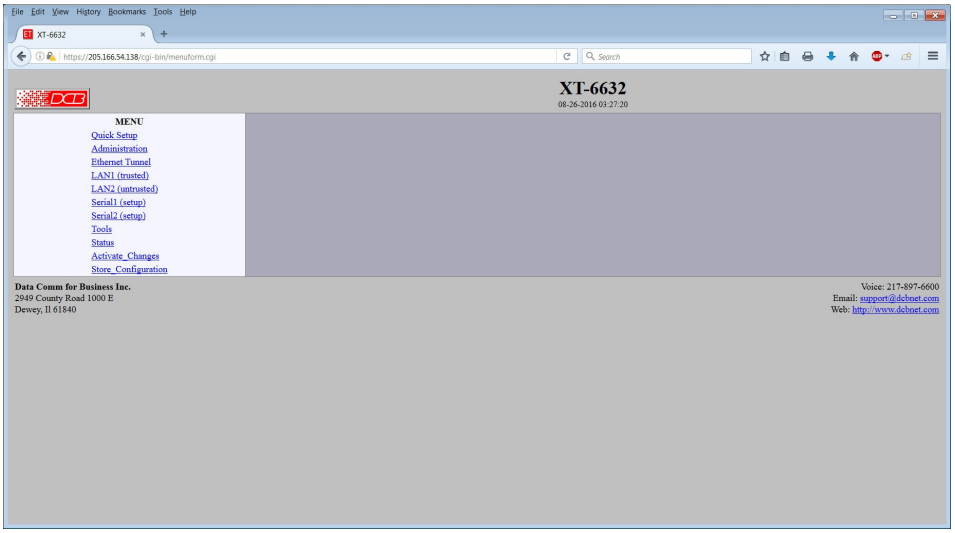
7. The bridge will now reboot.

2. Connect the Ethernet Cable

Connect a LAN cable from your hub or switch to Ethernet Port LAN1. Reboot the bridge with a power cycle. The bridge will now be available to any web browser on the same LAN segment. If your web browser does not see the bridge, verify that you do not have a proxy server configured in the browser and are using https instead of http for a secure connection. If so, properly configure the browser to bypass the proxy server for this URL. The bridge's default address is 192.168.0.1. This address must be appropriate for your local LAN and workstation, or step 1 above must be followed.

3. Verify the IP Address Configuration

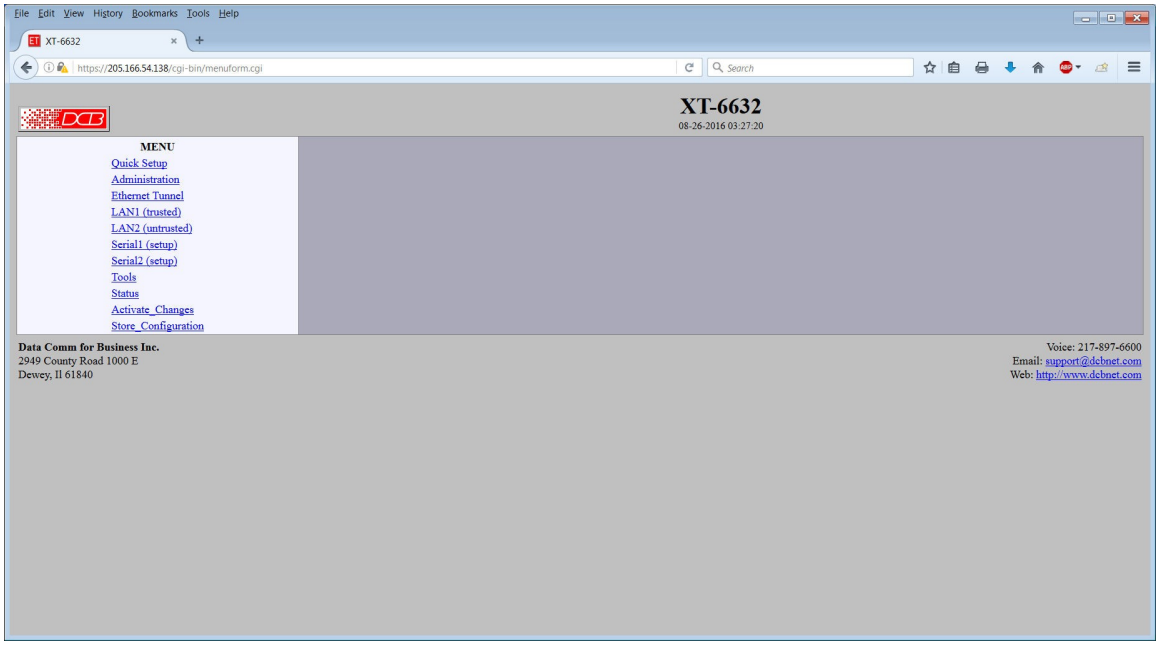
Enter the URL from step 1 (or https://192.168.0.1 if using the default address) into your web browser. The login screen below should be displayed.



Login Screen

Log in using the user name "admin" and no password (blank field). If this screen doesn't display, check the Troubleshooting Section in Chapter 6.

4. Enter Configuration Values



Initial Main Menu

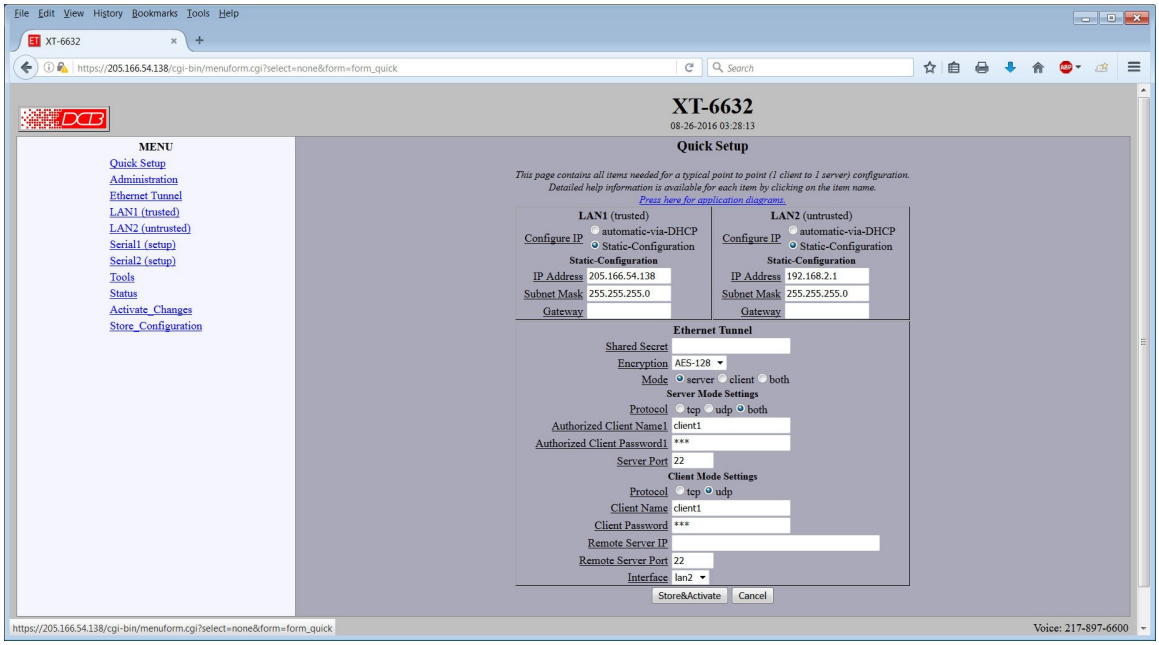
From this index screen, you can select a section on the left and will be taken to configuration screens for each bridge subsystem. You must enter configuration values specific to your installation.

5. Minimum Configuration

The minimum configuration items required for basic LAN-to-LAN bridging connection may all be entered using the Quick Setup screen.

1. Secure side ethernet configuration. Configure ethernet LAN1 to match your LAN.
2. Insecure side ethernet port configuration. The default is to use DHCP on Ethernet port B. It is usually appropriate to provide a fixed IP address for the server XT since the client XT must be configured with the server's IP address (or DNS name).
3. IP Tunnel Configuration. Defaults are acceptable for bench-testing, but not for actual use. Please change all items from default values. Default values for pass phrases and user names should NEVER be used.

These are all configurable from the initial "Quick Setup" screen (see Chapter 4).



Quick Setup Screen

Configure these items and the bridge is ready for use. Of course, you need to perform a similar installation for the companion bridge on the other LAN so it can do useful work.

Chapter 3
The Configuration Process

This Chapter describes the configuration management process on the XT-Family bridge using a Web Browser.

Overview

The XT-Family bridges contain a quite flexible configuration management system. By using this system correctly, one can remotely configure the bridge, save copies of that configuration to a PC, make configuration changes for later activation, and remote transfer firmware upgrades to the bridge.

There may be up to three configuration "images" in use at any time.

1. The ***active*** configuration. Normally, this is the configuration that was loaded from memory when the bridge was last booted. However it may have been changed since boot time as described below. This is the configuration that is currently running the bridge.
2. The ***pending*** configuration: This is the current configuration that was loaded form memory when the bridge was last booted WITH any changes made by using the configuration screens. This configuration is NOT the configuration running the bridge at present.
3. The ***stored*** configuration. This is the configuration that was last written to the bridge's non-volatile RAM. The next time the bridge boots, it will start running this configuration.

Note that any configuration transfer (with the Administration Configuration Transfer screen) is the *working* configuration. You can load a configuration file from the PC, then either activate it to test it. Or, store it without activation if you don't want to change the currently running configuration.

Using the Configuration Flexibility

When the bridge starts from a power-off condition, it loads an active configuration from its non-volatile memory. This active configuration is also copied to the working memory and is the "active" configuration.

Whenever the configuration screens are used to change values, **only** the *pending* configuration is changed… not the *active* configuration.

Using the configuration screens will change the pending configuration. You may change the active configuration by copying the pending configuration over it. This change is performed using the "Activate Configuration" screen. Going to this screen activates the pending configuration by copying the pending configuration over the top of the active configuration. This does not store the configuration in non-volatile memory. When the bridge is next reset or powered up, it will begin using the old stored configuration from before the changes were made and activate command clicked.

Using the "store configuration" screen will copy the pending configuration into Non-volatile memory. It will not cause this configuration to begin running the bridge. However, upon the next reset or power cycle, the bridge will begin using the stored configuration.

It is possible to activate the pending configuration using the Activate Configuration screen and then store the configuration using the Store Configuration screen. This two step process will cause all three configurations to be identical.

Configuration Process Examples

Example 1:

Make configuration changes, test them with Activate, then save them with Save.

This is the most commonly used method for changing the bridge configuration. It allows you to test the configuration prior to saving it. If, during the testing, you notice an abnormality; you can reset the bridge to return to the last good configuration.

Example 2:.

Make configuration changes, save them, reset the bridge to activate the changes.

This method allows one to configure the bridge via a bridge link that will not work using the new configuration. Make the changes to the pending configuration and save them. Your current session will not be affected, but when the bridge is reset, it will begin using the new configuration. This method is useful when you are configuring a bridge to use a new LAN address range while it is on the old LAN. It's also used when a dial-up PPP connection is the management path, and the new configuration will not allow that PPP connection.

Example 3:

Transfer a saved configuration to the bridge, save it, reset the bridge to activate the changes.

It is useful to transfer an existing bridge configuration to a PC text file for future use. Then if the bridge must be replaced, simply transfer that stored configuration to the new bridge.

If the PC is in the default IP address range of the new bridge (192.168.0.x subnet), then a new, XT-of-the-box bridge is easily configured using this method. Start the bridge, transfer a stored configuration file, and store it. When the bridge is restarted, it will have the proper configuration.

Saved Configuration Files

The saved configuration file is an encrypted file. Rather than configuring a new bridge from defaults, you may wish to save this configuration, then transfer the it to a different bridge, then modify it on the new bridge.

This method is ideal for automating the configuration of many bridges in a large corporate environment.

Chapter 4
Configuration

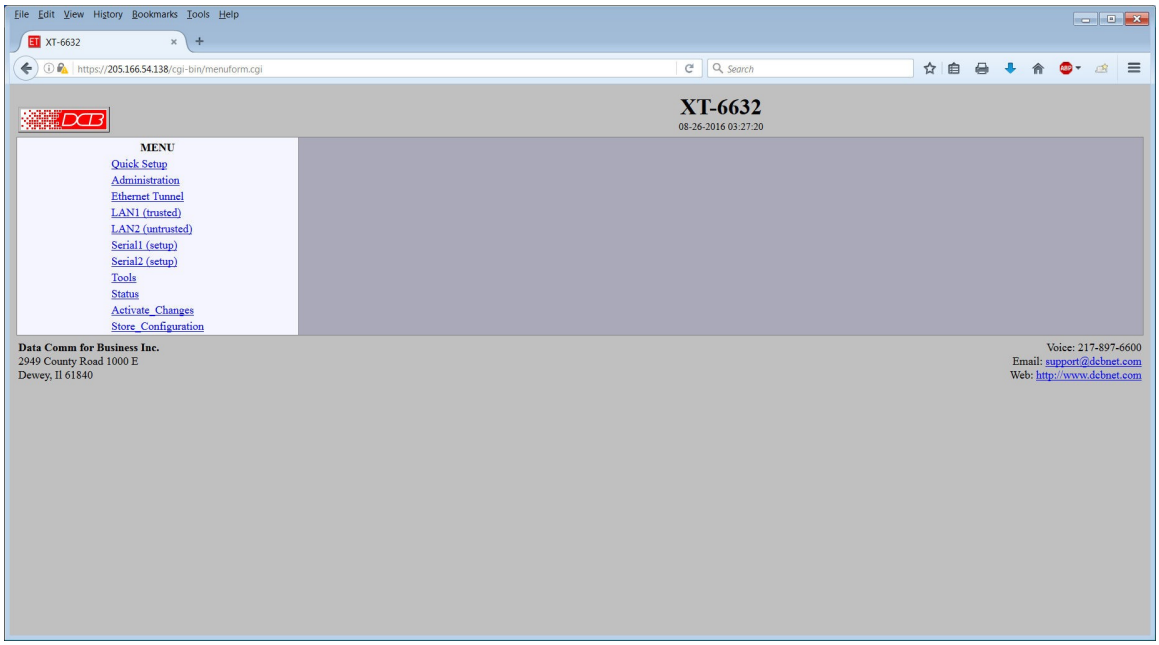
This Chapter describes configuration screens and some configuration hints for the EtherSeries XT-Family Bridge

Overview

The XT-Family bridge is configured using forms displayed on a web browser. In this chapter, we illustrate all entry forms, and describe their use. This is not a tutorial on IP, subnetting, bridging, or routing. Familiarity with IP and related information is required before you can configure any ethernet product.

All configuration screens are accessed from the main index screen shown below. They are divided into sections with only one layer of screens below the top level.

Configuration screens should only be made available via the trusted interface. This default operation may be changed during configuration, but it is highly recommended that configuration be locked to the secure interface. Most models require a secure web browser connection for configuration (https://) by default.

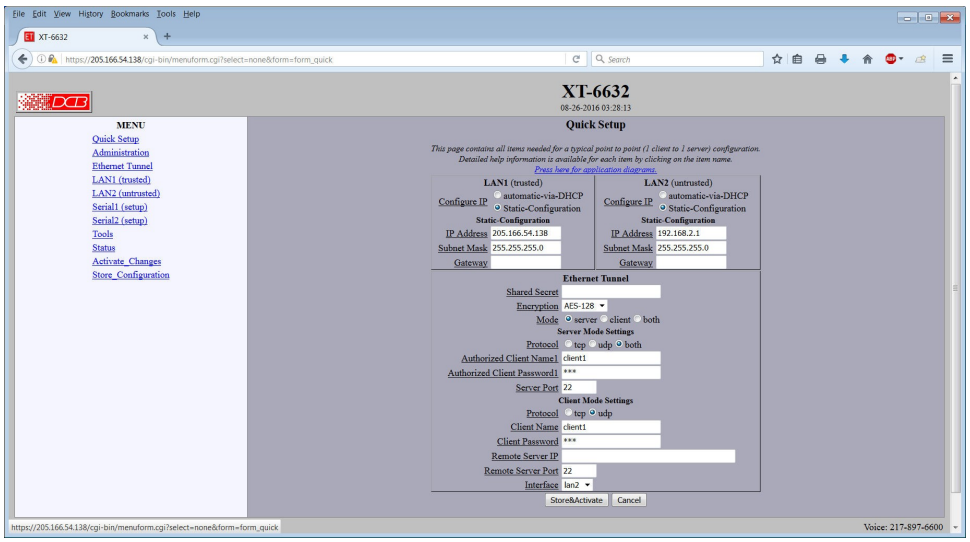


XT-6632 Main Screen

From this index, click on a menu keyword to open the appropriate screen. In this manual, screens are discussed in the order shown on the index screen.

Note that some screens are model specific, and some models do not contain all screens shown.

Quick Setup Configuration Screen



Quick Setup Configuration Screen

For a simple point-to-point bridge setup using two copper ethernet interfaces, all needed values may be entered on this single screen. However, if single-port configuration is required, the untrusted ports must be disabled on their Mode configuration screens. Additional features and values are configured on different screens.

There is also a link from this page that shows the most commonly used application diagrams on the help screen.

Fields

LAN1 (Trusted)

- Configure IP
  Select DHCP or a static configuration. If DHCP is selected, the static-configuration values are ignored.
- IP Address
  An IP address is a numeric identifier given to an interface. It consists of four 8-bit numbers and is represented in a dotted notation. An example of an IP address is "192.168.0.10". An Ethernet IP address must be unique within your network. If you are directly connected to the Internet, it must globally unique.
  This field is not used if DHCP Client has been enabled. The DHCP server will assign the IP address.
- Subnet Mask
  A subnet mask is a bit mask applied against the IP address. It specifies which portion of the IP address is the subnet identifier and which portion is the host identifier. For example, many subnets have a mask of 255.255.255.0. This means the first 24 bits of the address is the subnet identifier and the last 8 bits is the host identifier.

  This field is not used if DHCP Client has been enabled. If using DHCP, the subnet mask will be assigned by the DHCP server.
- Gateway

The Gateway specifies the address of the gateway router on the local subnet. Packets destined for a host not on the local subnet are forwarded to the gateway router. The LAN1 gateway is normally left blank.

The tunnel uses policy-based routing rules which allow each interface to have a gateway router defined. Routing decisions take into account the source IP address when selecting a gateway. Instances where a source address has not been established, such as when initiating a connection, ping, etc, the tunnel will give priority to LAN2's gateway.

LAN2 (Untrusted or public side)

- Configure IP
  Select DHCP or a static configuration. If DHCP is selected, the static-configuration is ignored.
- IP Address
  An IP address is a numeric identifier given to an interface. It consists of four 8-bit numbers and is represented in a dotted notation. An example of an IP address is "192.168.0.10". An Ethernet IP address must be unique within your network. If you are directly connected to the Internet, it must globally unique.
  This field is not used if DHCP Client has been enabled. The DHCP server will assign the IP address.
- Subnet Mask
  A subnet mask is a bit mask applied against the IP address. It specifies which portion of the IP address is the subnet identifier and which portion is the host identifier. For example, many subnets have a mask of 255.255.255.0. This means the first 24 bits of the address is the subnet identifier and the last 8 bits is the host identifier.

  This field is not used if DHCP Client has been enabled. If DHCP is used, the subnet mask will be assigned by the DHCP server.
- Gateway

  The Gateway specifies the address of the gateway router on the local subnet. Packets destined for a host not on the local subnet are forwarded to the gateway router.

  The tunnel uses policy-based routing rules which allow each interface to have a gateway router defined. Routing decisions take into account the source IP address when selecting a gateway. Instances where a source address has not been established, such as when initiating a connection, ping, etc, the tunnel will give priority to LAN2's gateway.

Ethernet Tunnel

Shared Secret
The shared secret provides the initial level of privacy and is used to authenticate all bridges. All bridges participating in the private network must have the same shared secret. This secret phrase is used to generate the AES key used to cypher the initial communications. The secret phrase may be up to 51 characters in length. Do not use a quote or backslash character in the phrase. Best security requires a long, random shared secret.

Encryption
This options selects the encryption method for data passed between the tunnels. Encryption is available in 128 bit, 192 bit, or 256 Bit AES. AES, also known as Rijndael, is a NIST approved encryption method. “None” disables encryption and is used when encryption security isn't required.

Mode

Server, Client, or Both. Select the mode for this unit. It is permissible for a tunnel to be both a server and client simultaneously.

Server Mode Settings:

Protocol

This option configures the server to operate in TCP mode, UDP mode, or both TCP and UDP mode.

Authorized Client Name1
The name may be up to 51 characters in length. Do not use a quote or backslash character in the phrase. If blank, this entry is ignored.

Authorized Client Password1

The password may be up to 51 characters in length. Do not use a quote or backslash character in the phrase. If blank, this entry is ignored.

Server Port

The TCP/IP or UDP/IP port to listen to when server mode is enabled. If the server is placed behind a firewall or NAT router, then the router must be configured to allow or forward to this port.

Client Mode Settings:

Protocol

This option configures the client to operate in TCP mode, UDP mode, or both TCP and UDP mode.

Client Name

This is the client name sent to the server tunnel when authenticating. The client must use a matching name. The client name may be up to 51 characters in length. Do not use a quote or backslash character in the phrase.

Client Password

This is the client password used to authenticate the client to the server. The server must have a matching password in its table of Authorized Remote Clients. The password may be up to 51 characters in length. Do not use a quote or backslash character in the phrase.

Remote Server IP

The host name or IP address of the server tunnel. That is the address this client will connect to. It may be the outside address of a port forwarding router at the server.

Remote Server Port

The UDP/IP or TCP/IP port to connect to when client mode is enabled. The server shouldbe listening on this port. It may be the outside port of a port forwarding router at the server.

Notes

In simple applications, the Quick Setup screen may be the only screen requiring configuration.

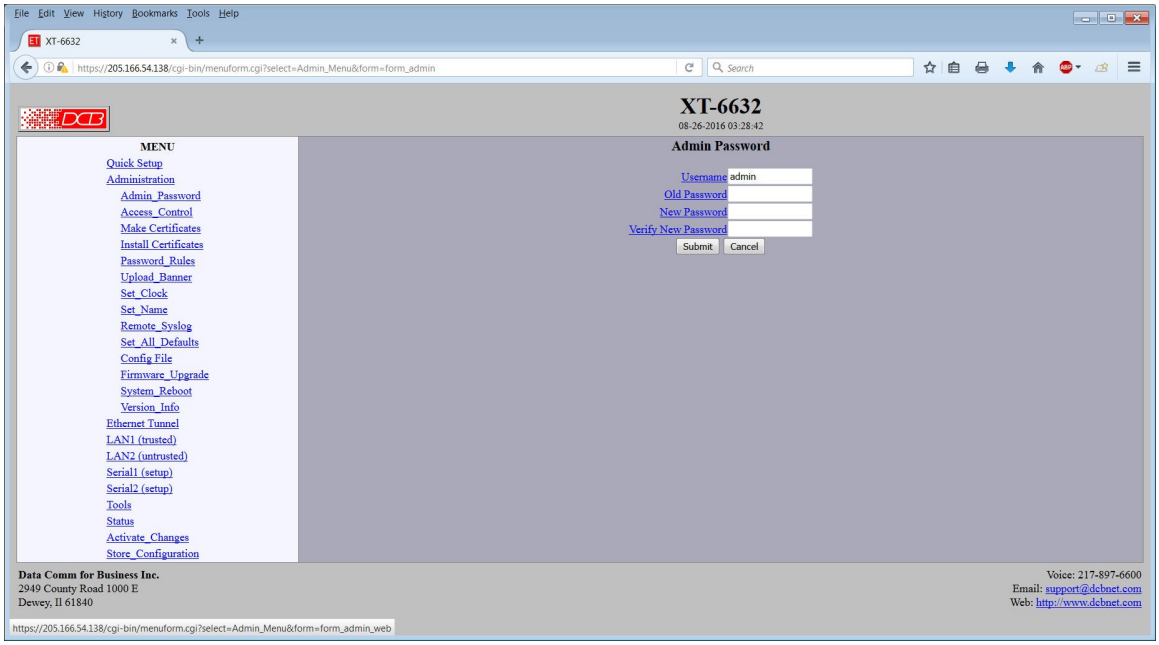
The XT should never be used in actual applications without changing all passwords. When used as a non-encrypting bridge, there is no security on the link between the XTs, and all traffic may be monitored by any node in the link, just as with any other bridge or router.

If the XT is to be used in a single-port application, LAN2 should be disabled on the LAN Mode screen.

Administration

The Administration section contains screens used to configure system-wide settings and perform a few high level operations.

Admin Password



Admin Password Screen

By default, the XT web server screens are available ONLY via the secure side of the bridge.

Normally, access to the XT's Web Server is protected by HTTP Basic Authentication and uses the secure web server. This is a simple methodology where the Web Server will require a Web Browser to provide a username and password for each page requested. The Web Browser will typically ask the user to enter the username and password once, then will remember it for the duration that the Web Browser is running.

The Administration Password screen allows you to change the user name and password for the bridge administrator. This is the only user allowed to configure the bridge. **If you forget the administrator name or password, the bridge can only be configured by returning it to factory defaults as described in the quick start chapter. The XT-3305 can be be cleared by using the reset button.**

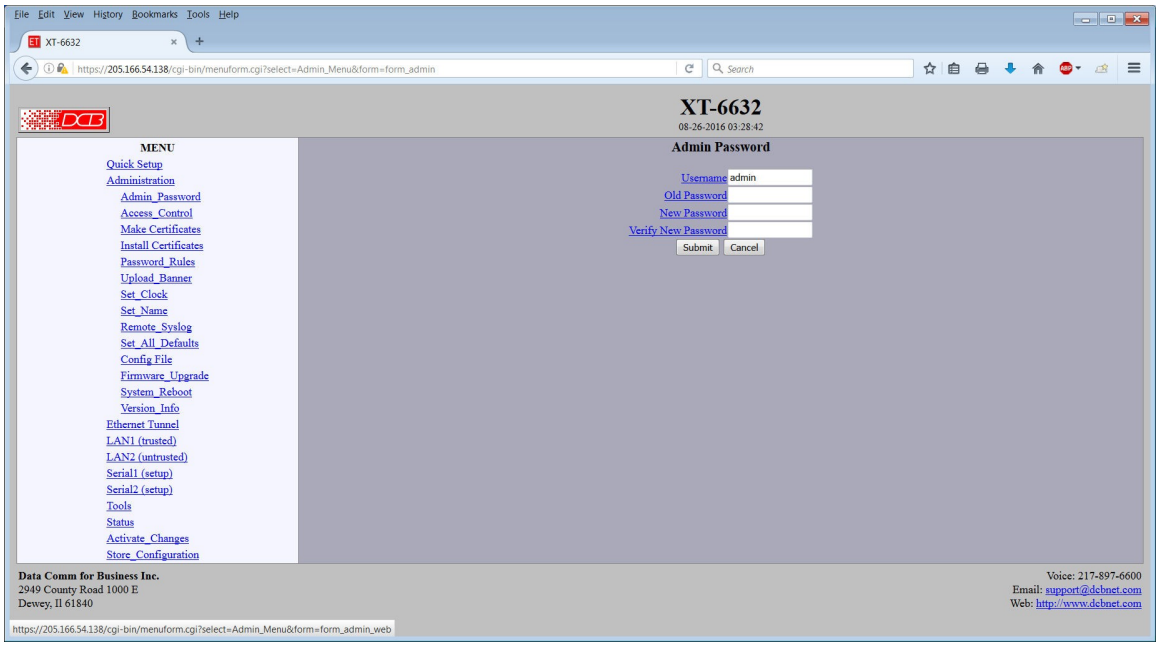
Fields

- User Name
  This field may be a string of 0 to 15 printable characters. Do not use space or control characters. If you leave this field blank, you will need to enter a blank username during authentication.
- Old Password
  In order to change the username and password, you must know the old password. When making a change, enter the current password in this field.
- New Password
  When changing the username and password, this field provides the new password. It may be a string of 0 to 15 characters. If you leave this field blank, you will need to enter a blank password during authentication.
- Verify New Password
  Retype the password to verify that it was correctly entered.

Notes

- If you forget your username or password, you can use the Serial Port Setup to erase the current settings and return the unit to factory defaults.
- HTTP is not available in the XT series. All web browser communication is via HTTPS.

Admin Access Control



Administrative Access Control Screen

Access Control allows you to place further restrictions on access to the XT's internal web server.

Fields

- Web Server Port
  This is the TCP Port to use for the internal Web Server. Typically it is set to port 443. However you may set it to any value between 1 and 65535.

  There are several reasons that you may want to change the web server port. By changing it to a non-standard value, you slightly reduce the chance that a random attacker will find the XT's web interface and attempt to break in. A different port may be needed to accommodate local firewalling.

  If you change the web server port number to any value other that 443, remember that you will have to include the port number in your URL. For example, https://192.168.0.1:7995 OR https://192.168.0.1:7995 .

- Require Certificates (Applies only to XT-6606 and XT-6632)
  This option enables certificate based authentication of web browsers attempting to connect to the tunnel's internal web server. The browser must present the appropriate certificate, otherwise access will be denied. See the help section on making and installing certificates.

  Certificate based authentication is strongly recommended if access to the tunnel's web server is allowed via a public interface. Most customers do not use certificate based web access.

- Authentication Method
  This option allows selection between two different methods of authenticating web access. HTTP Basic is the method built into web servers and web browsers. A user name and password is required to access each web page. Once the user has entered the credentials into the web browser, the web browser will cache the information and automatically provide them to the web server. A disadvantage of HTTP Basic Authentication is that it has no mechanism to re-authenticate a user after a period of time. This creates a security risk if the user fails to close their web browser.

  CGI Session is an alternate authentication method built using CGI scripts on the web server. It implements session timers and will require the user to re-authenticate after the session has been idle for some period of time.

- CGI session Idle (minutes)
  This option only applies when CGI Session authentication is enabled. It configures the idle time-out period for a session. Once a web session has been idle for the configured time-out period, the user will need to re-authenticate with the web server. The time is specified in minutes and may range from 5 minutes to 120 minutes.

  There is no option to disable the timer. If no time-out period is desired, please use HTTP Basic authentication.

- Interface LAN1 and LAN2 Web Access
  These options allow you to block web access through the specified interface. If you are using the tunnel to bridge across a public network, you are strongly advised to disable web access from the interface attached to the public network.

- Accepted Web IP Source Address
  This table allows you to control what hosts or networks have access to the XT's web server. If empty, any host may access the unit.

  Entries are made by specifying a Target and Netmask. For example, if you want to allow only the host 192.168.10.16 access, you would enter:
  Target: 192.168.10.16 Netmask:255.255.255.255.

  If you wanted to allow access to all hosts in the range 192.168.10.1 to 192.168.10.255, you would enter:

  Target: 192.168.10.0 Netmask: 255.255.255.0

- Target
  Host or Network address.

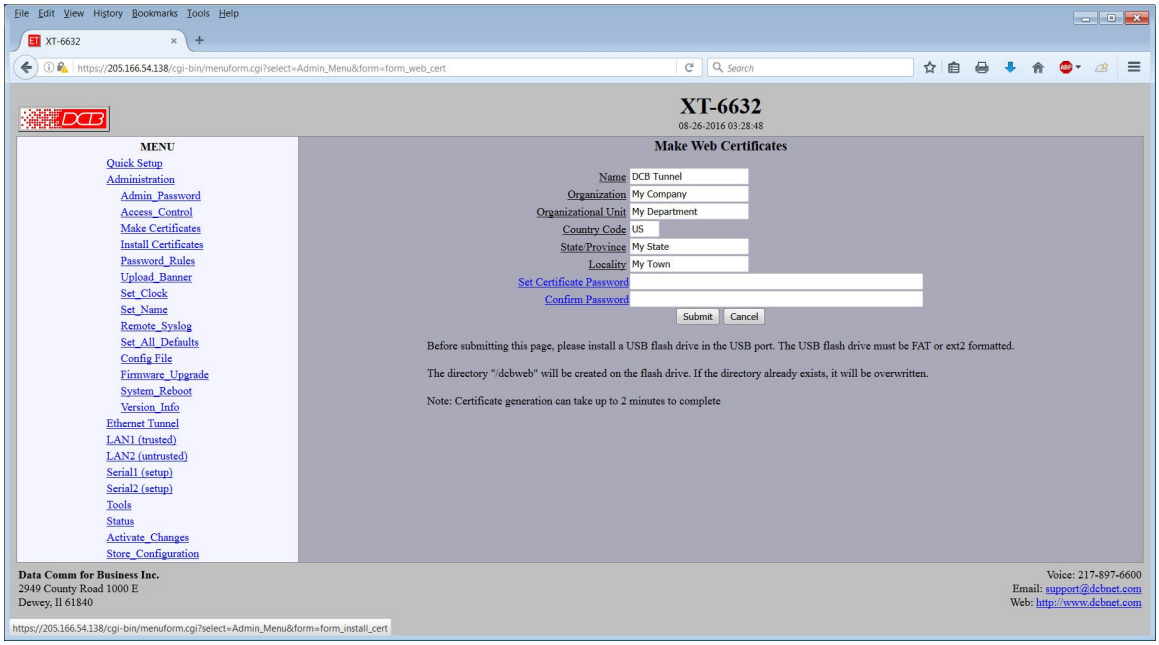
- Netmask
  If blank or set to 255.255.255.255, target is assumed to be a host address. Otherwise, target is treated as a network address.

- Respond to Ping
  This item allows you to block ping requests to the XT. Ping is a valuable tool for diagnosing network problems, but can also become a security problem. Disabling ping causes the XT to not respond to ping requests for one of its IP addresses. It has no effect on the XT's passing of ping request and responses from other network nodes.

Notes

Remember to submit the change by clicking the “SUBMIT” button.

Make Web Certificates



Make Web Certificates Screen

The tunnel's secure web server operates using the SSL protocol. SSL allows for the use of x509 certificates to identify and authenticate web servers and web browsers. You may use this form to generate a pair of x509 certificates. One to identify your tunnel's web server and the other to identify your computer's web browser.

This form only generates the certificates, writing them to a USB Flash Drive inserted into one of the tunnel's USB ports. Separate steps are required to install the certificates into the tunnel's web server and your computer's web browser. For more information, see installing web certificates.

Four file will be written to the directory:

```
dcbweb/
   wbrowser.p12 - browser certificate file in PKCS12 format
   wbrowser.pem - browser certificate file in PEM format
   wserver.pem  - server certificate file in PEM format
   wserver.key  - server private key file
```

Fields

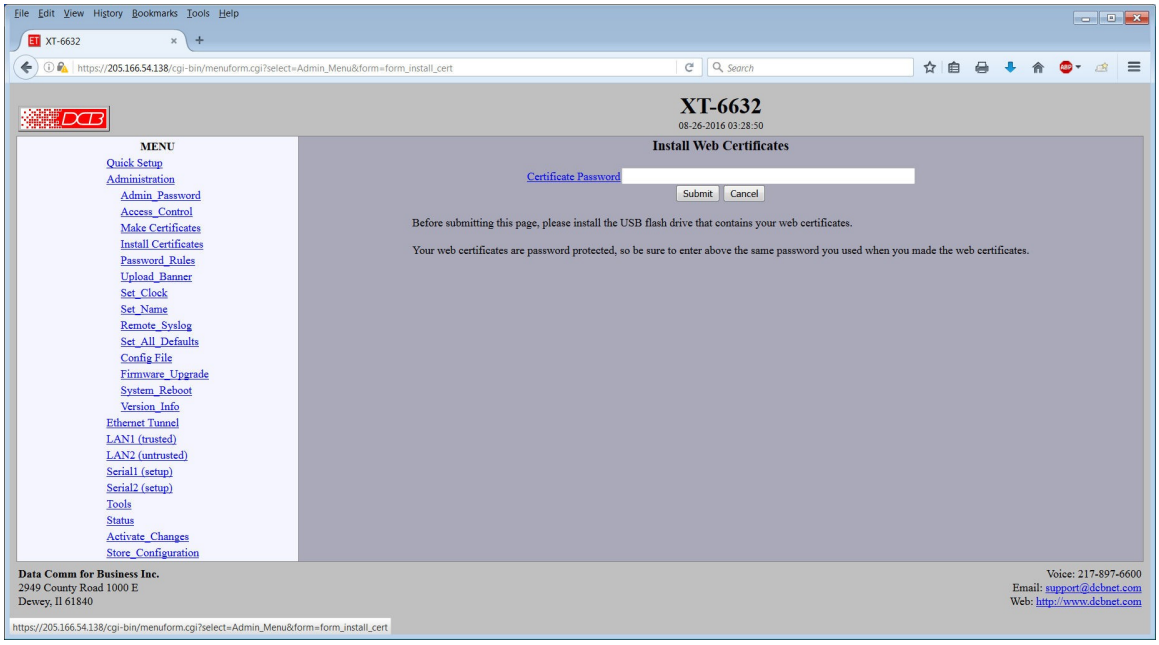
- Name
  The common name given to the certificate. The supplied name will be appended with the word "Server" for the server certificate and the word "Browser" for the browser certificate. Name may be 1 to 64 characters in length, limit to alph-numeric characters.
- Organization
  The organizational name given to the certificate. It may be 1 to 64 characters in length, limit to alph-numeric characters.

- Organizational Unit
  The organizational unit name or departmental name given to the certificate. It may be 1 to 64 characters in length, limit to alphanumeric characters.
- Country Code
  The country code given to the certificate. It is 2 characters in length, limit to alphanumeric characters.
- State / Province
  The State or Province name given to the certificate. It may be 1 to 64 characters in length, limit to alphanumeric characters.
- Set Certificate Password
  The password used to protect the private keys stored in the certificate. It may be 1 to 64 characters in length, limited to alphanumeric characters. You will need to know this password when you install the certificates.
- Confirm Password
  Re-enter the password for confirmation.

Notes

Remember to submit the change by clicking the “SUBMIT” button.

Install Web Certificates



Install Web Certificates Screen

This form will allow you to install two x509 certificates into the tunnel's secure web server. One certificate is used to identify the web server. The second is used to verify the identity of the web browser. To install these certificates, insert the USB Flash drive that contains the previously generated certificate files into the tunnel's USB port. Enter the password used when the certificates were created and submit the page. The necessary files will be imported from the USB Flash drive. Activate and store the configuration to make

them permanent. *You may want to hold off storing the changes until you have successfully imported the certificates into your web browser.*

After the new certificates are activated, the tunnel's web server will refuse to communicate with your web browser. You will need to import the certificate files from the USB Flash Drive into your web browser. The actual method depends upon your browser and version, but the method for Internet Explorer and Firefox is described below.

```
- Insert the USB Flash Drive into your computer.
- For Firefox:
      Go to "Edit/Preferences/Advanced/Security".
- For Internet Explorer:
      Go to "Tools/Options/Privacy".
- Click on the "View Certificates" button.

Browser Certificate
- Make sure the "Your Certificates" tab is selected.
- Press the "Import" button.
- You will be prompted for your Master Password.  The Master
  password is for protecting your web browser's certificates.
  If this is the first time you have imported a certificate,
  you will be asked to create a password.
- Select the file "dcbweb/wbrowser.p12" from the USB drive.
- You will be prompted for the password used encrypt the
  certificate.  Enter the same password you used when you
  generated the certificates.

Server Certificate
- Select the "Web Sites" tab.
- Press the "Import" button.
- Select the file "dcbweb/wserver.pem" from the USB drive.
- After import, highlight the server's certificate.
- Press the "Edit" button.
- Select "Trust the authenticity of this certificate"
- Press "OK"
```

Your browser should now be able to communicate with the server. It is normal to get a "Domain Name Mismatch" warning when you connect to the server. However, you should not get a "Website Certified by an Unknown Authority" or an "Untrusted Website" warning. If you do, it indicates that certificate presented by the device does not match the one stored in your web browser and that you may be communicating with an impostor device.

Note: It is permissible to install the same pair of certificates to multiple devices allowing all to be administered with the same set of certificates.

Fields

- Certificate Password
  The password to use to decrypt the private key stored in the certificate files. This must be the same password used when the certificates files were generated.

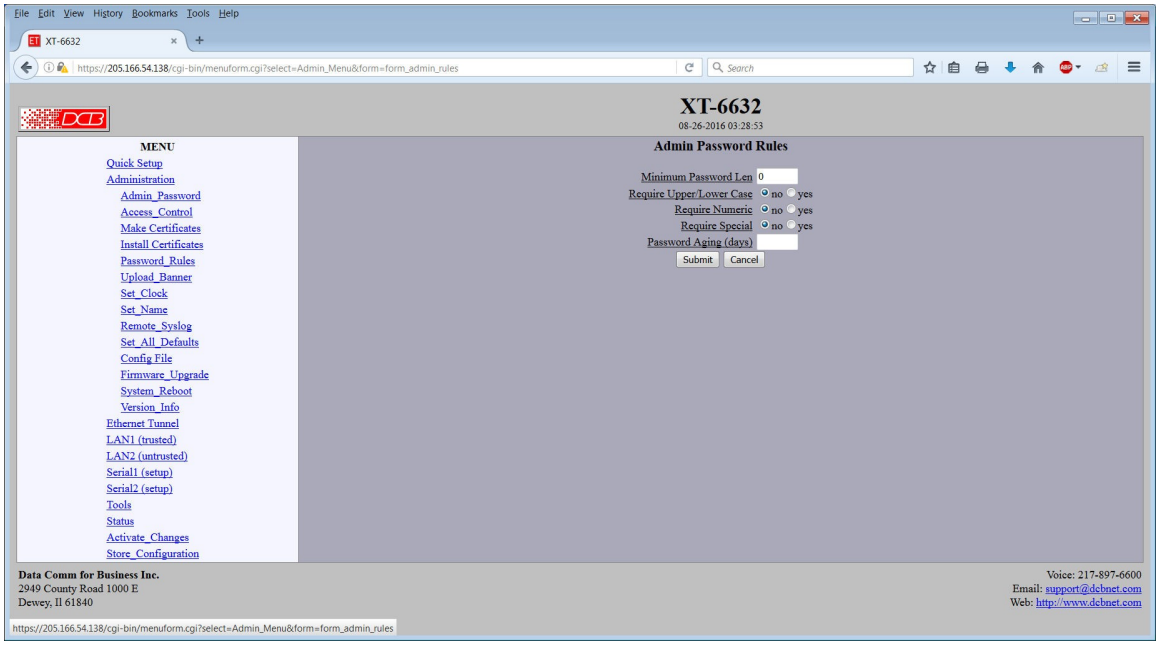
Notes

Before submitting this page, please install the USB flash drive that contains your web certificates.

Your web certificates are password protected, so be sure to enter above the same password you used when you made the web certificates.

Remember to submit the change by clicking the “SUBMIT” button.

Password Rules



Admin Password Rules Screen

Access Control allows you to place further restrictions on access to the XT's internal web server.

Fields

- Minimum Password Length
  This option sets the minimum password length in characters. It may range from 0 to 15 with 0 indicating that a blank password is allowed.
- Require Upper/Lower Case
  When set to *yes*, the password must contain at least 1 upper case character and at least 1 lower case character.
- Require Numeric
  When set to *yes*, the password must contain at least 1 numeric character (0 - 9).
- Require Special
  When set to *yes*, the password must contain at least 1 special character, such as a punctuation mark or

a symbol.

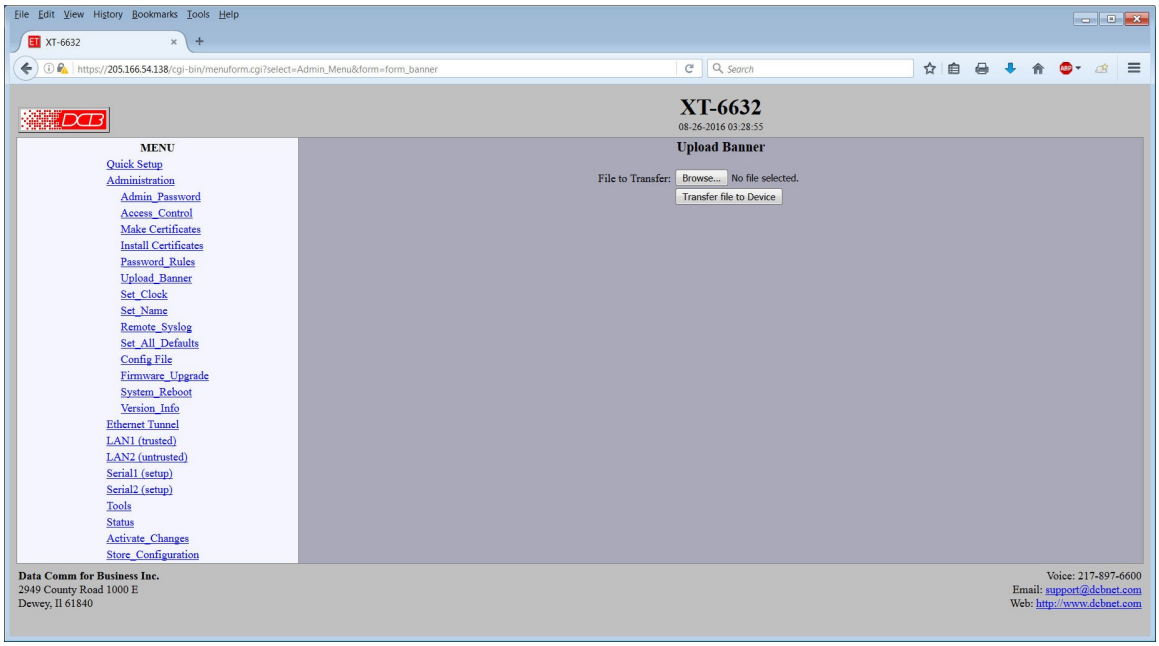
Note: space characters and control characters may not be used in the admin password.

- Password Aging
  This option enables a password aging feature. When enabled, the user will be required to change the password when the password has reached the specified age. A blank or zero value disables the feature. The valid range is 1 - 365 days.

Notes

Remember to submit the change by clicking the “SUBMIT” button.

Upload Banner



Upload Banner Screen

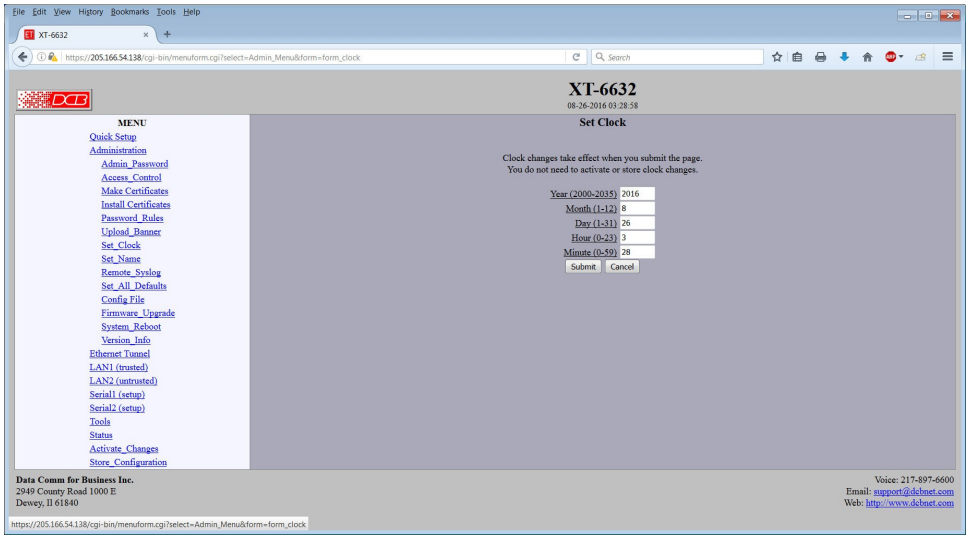
This screen allows you to transfer a banner file to the bridge. The file is a text file and it may contain simple html formatting.

Fields

- Browse
  Browse to a file to upload.
- Transfer File to Device
  Click to transfer the banner file.

Notes

Set Clock



Set Clock Screen

This form allows you to set the XT's software clock. The setting will take effect when you "Activate Changes". All models include a client for NTP. We recommend using NTP for time synchronization.

Fields

Year Year in the range 2000 to 2035.

Month Numeric value of month in the range 1 to 12.

Day Day of month in the range 1 to 31.

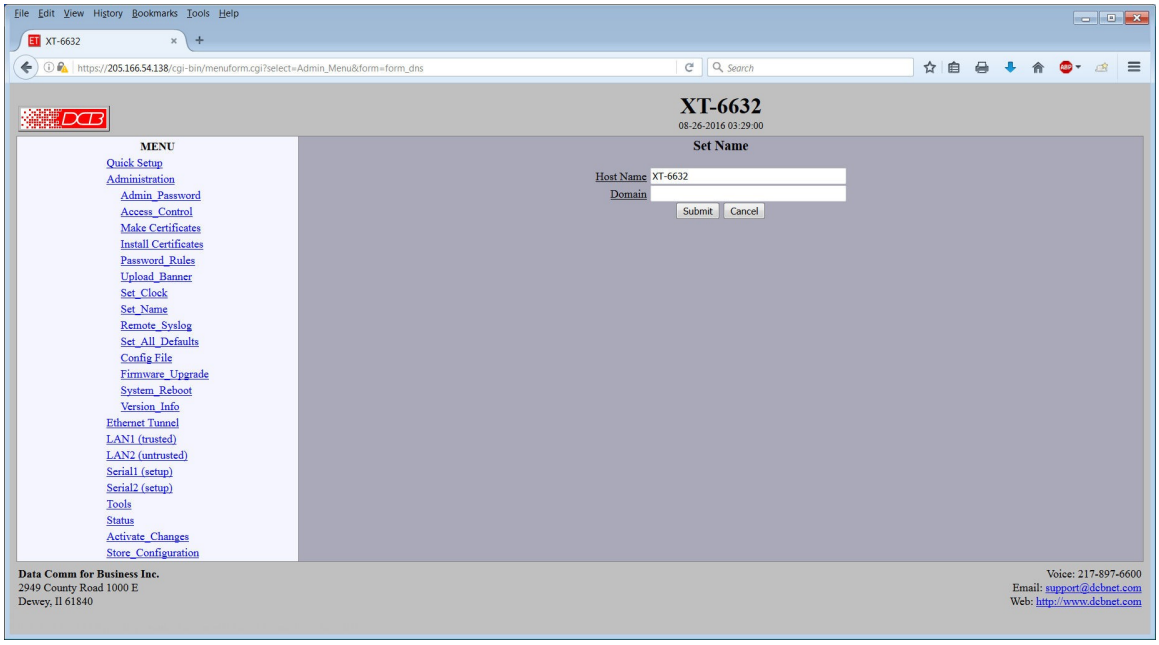
Hour Hour of the day in the range 0 to 23.

Minute Minutes in the range 0 to 59.

Notes

- If you save the time to non-volatile memory, the clock will be set to the specified time at each reboot.
- Some models of the XT do not contain a real-time clock, nor have the ability to remember the current time across reboots. The software clock is used for time stamping log entries.
- The default values shown on this screen for those products are the “boot” values… not the current time.

Set Name



Set Name Screen

This form allows you to set the XT's host name and domain.. The setting will take effect when you "Activate Changes". Configuring each unit with a unique name is recommended.

Fields

Host Name

The name given to the bridge. If you enter a name, it will be displayed as the title of the web pages.

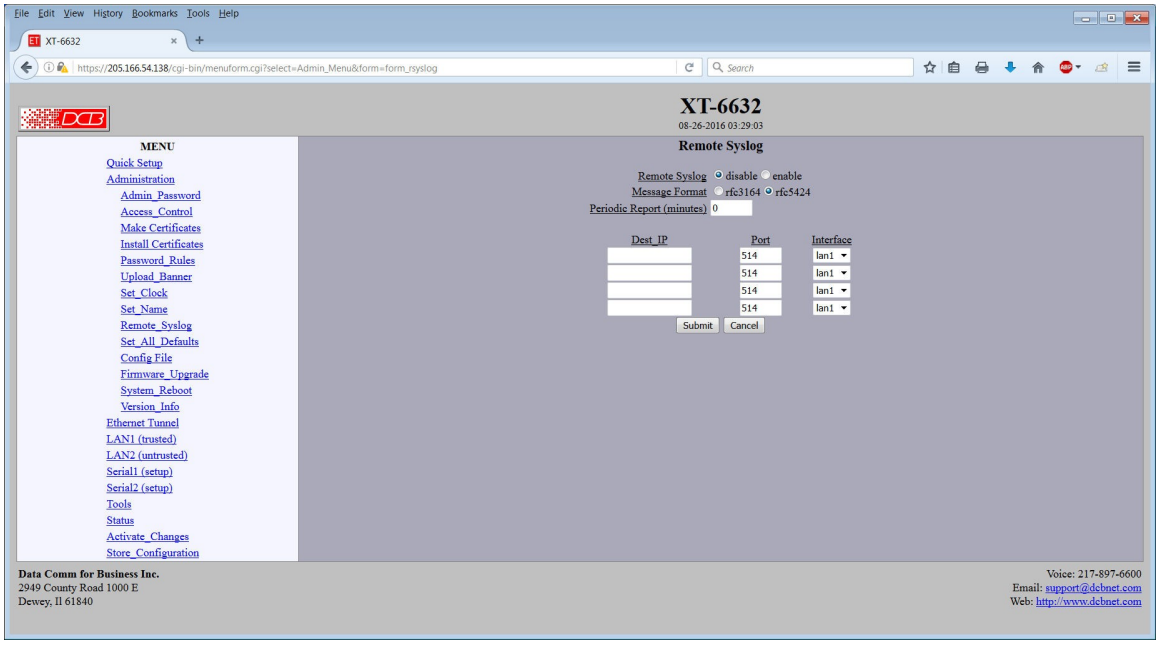
Domain

The name of the local domain. For example: widgets.com

Notes

- If used, these names must be appropriate for your DNS system.

Remote Syslog



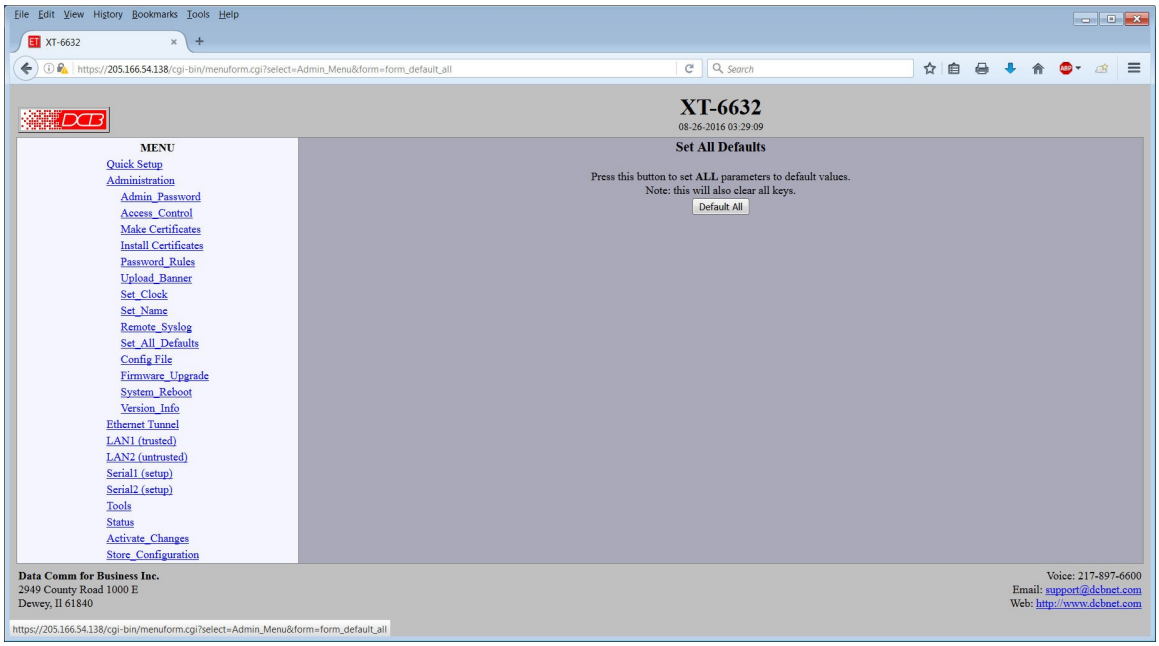
Remote Syslog Screen

This screen is used to configure remote syslog(Rsyslog) functionality. Both rfc-3164 and rfc-5424 formats are available. The syslog server may be on reached on either the trusted or untrusted LAN interface. If it's on the untrusted port, messages are sent in the clear. To syslog to a server at another bridged site, select the trusted interface.

Fields

- Remote Syslog
  Enable/Disable sending log messages to a remote syslog server.
- Messsage Format
  The format of the messages sent to the remote syslog server. If you are unsure which format to use, one of the distinguishing features is the format of the timestamp. For example, RFC3164 would format the time as *"Feb 1 13:55:25"* where RFC5424 would format the same time as *"2015-02-01T13:55:25"*.
- Periodic Report (Minutes)
  This option will cause a periodic syslog message to be sent to the remote syslog server. The time is set in minutes. The value 0 disables the feature.
- Device IP
  The IPv4 address of a remote syslog server. Host names are not allowed.
- Destination Port
  The UDP port number of the remote syslog server. UDP port 514 is the port normally reserved for rsyslog.
- Destination Interface
  The interface to use when sending log messages to the server

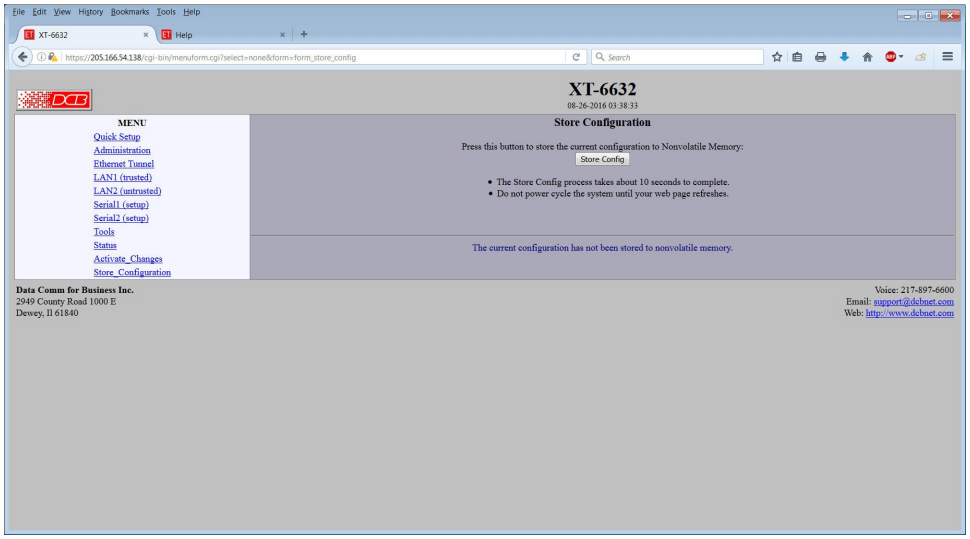
Set All Defaults



Set All Defaults Screen

This form will allow you to set all tunnel parameters to their default value. **Before you "Activate Changes", you should configure the interface that you are using to access the tunnel. Otherwise, all interfaces except LAN1 will be disabled and LAN1 will be configured with the IP address of 192.168.0.1.**

Configuration File



Configuration File Screen

This form will allow you to copy the bridge's configuration to a file on your PC. You can also use the form to transfer a configuration file from your PC to the bridge. The file is encrypted.

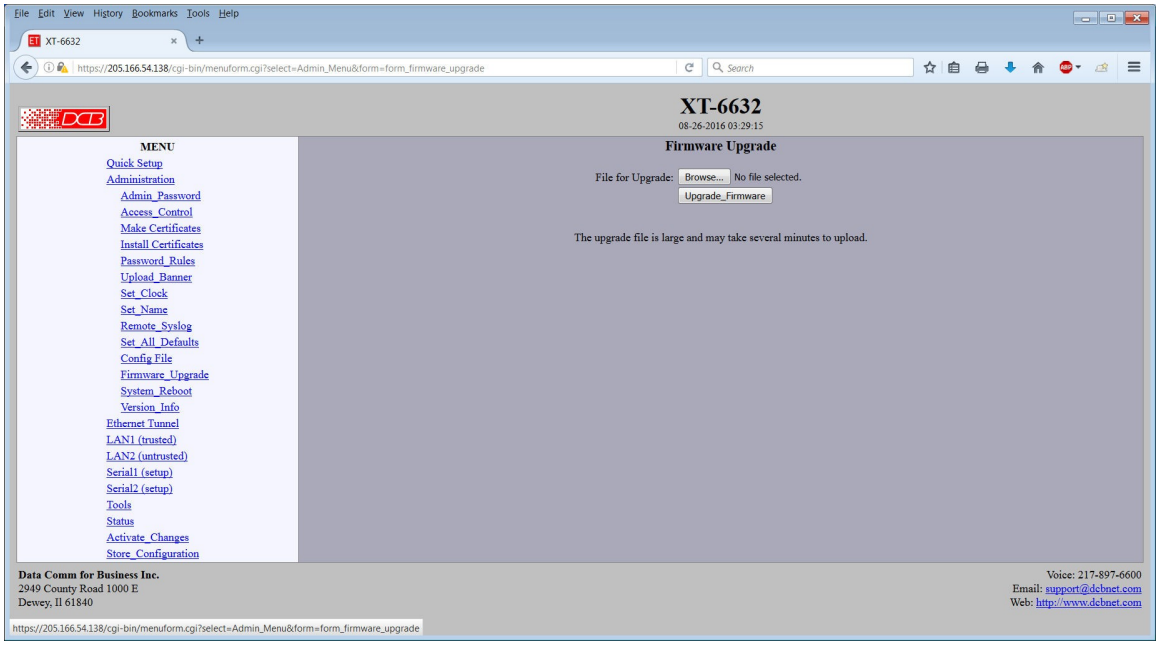
Fields

- Set Password
  This is the password used to encrypt the configuration file on your PC. This password is not used for any other purpose on the bridge. **It will be required to retrieve the configuration file later.**
- Confirm Password
  Re-enter the password
- Transfer file to PC
  Transfers the configuration to a PC file. Your operating system will then allow you to select a file name.
- File to Transfers
  Browse to the configuration file you wish to retrieve.
- Password
  Enter the password for the configuration file to be retrieved.

Notes

- The configuration file is encrypted with a password that is only used for storing and retrieving the configuration file.
- You may save multiple configuration files on the PC by using different names for them.
- After transferring a configuration file to the bridge, you may either activate the changes (with the activate screen), or store the changes (with the store configuration screen). If you activate the changes, the bridge will immediately begin using the new configuration. If the changes are stored, the bridge will use the new configuration only after a reboot or reset.
- If you activate the new configuration, first be sure that you can access the bridge using its new configuration. Otherwise, it may be necessary to return to the old stored configuration with a reset.

Firmware Upgrade



Firmware Upgrade Screen

This form will allow you to load new firmware into the XT. The firmware will be saved to non-volatile memory, replacing the current firmware.

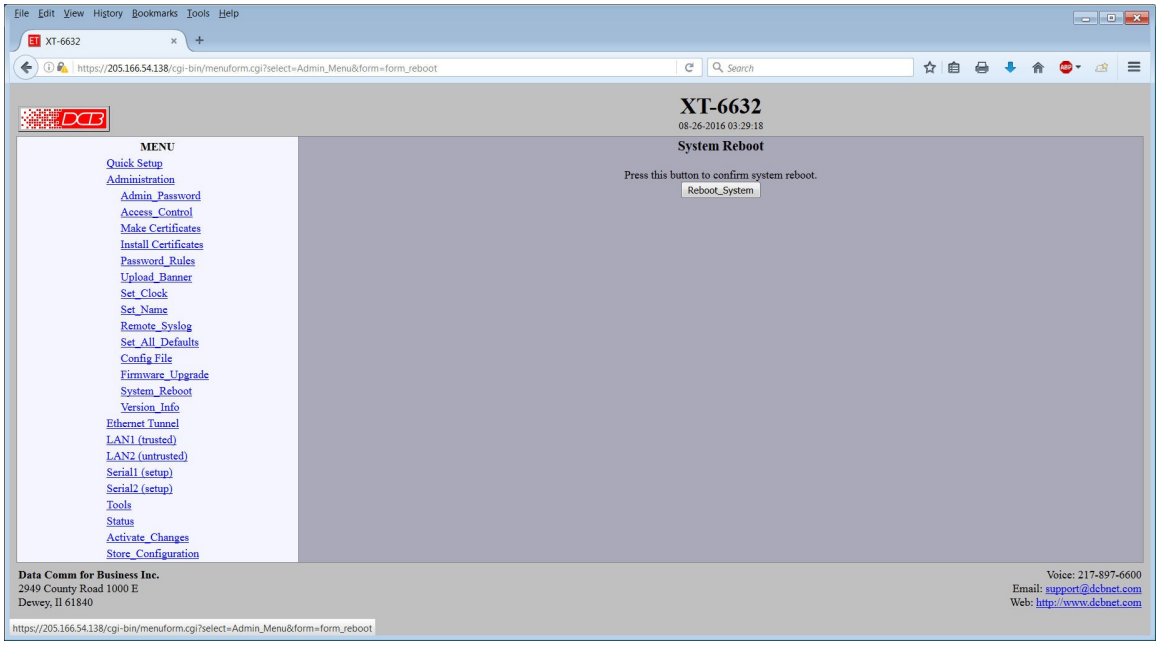
Fields

- File Name
  This is the name of the firmware image file to be transferred to the bridge.
- Upgrade Firmware (action)
  Pressing this button transfers the firmware image to the bridge and upgrades it.

Notes

You should only use a firmware image obtained directly from DCB. To obtain updated firmware, contact DCB support by phone at 217-897-6600 or email support@dcbnet.com .

System Reboot



System Reboot Screen

This form will allow you to reboot the XT. **If you made configuration changes that have not been saved to non-volatile memory with the "Store Configuration" menu option, they will be lost.**

This is a way to revert back to your previously stored configuration.

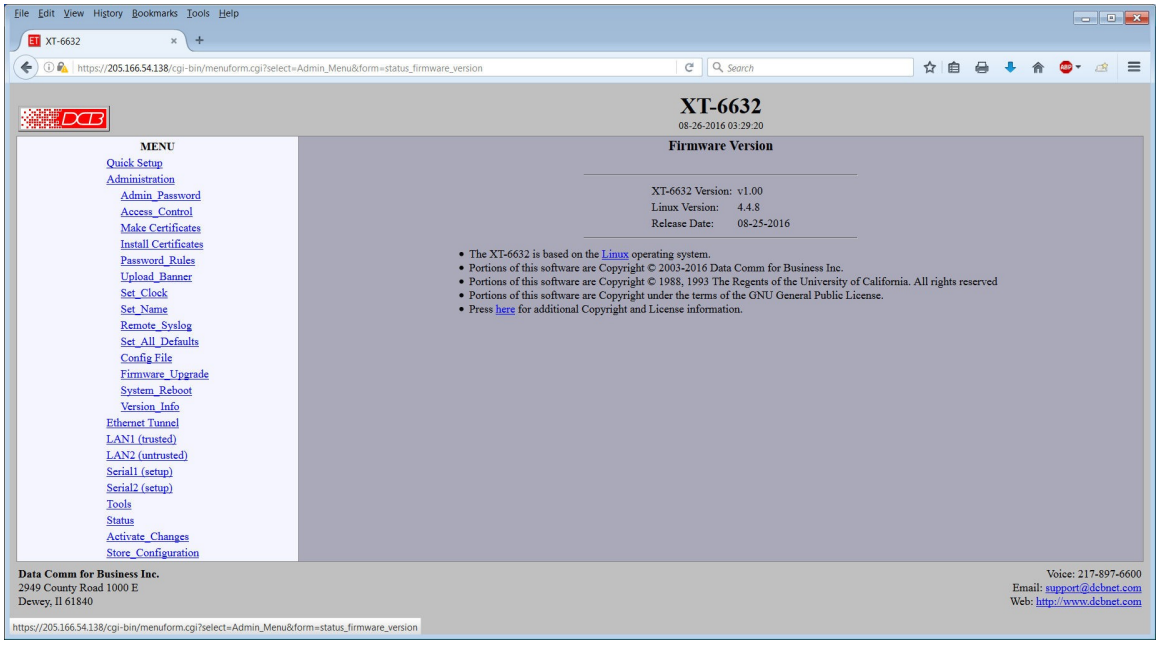
Fields

- Reboot System (action)
  This causes the bridge to reboot and use its stored configuration.

Notes

- The current configuration is not retained unless it has been previously stored.

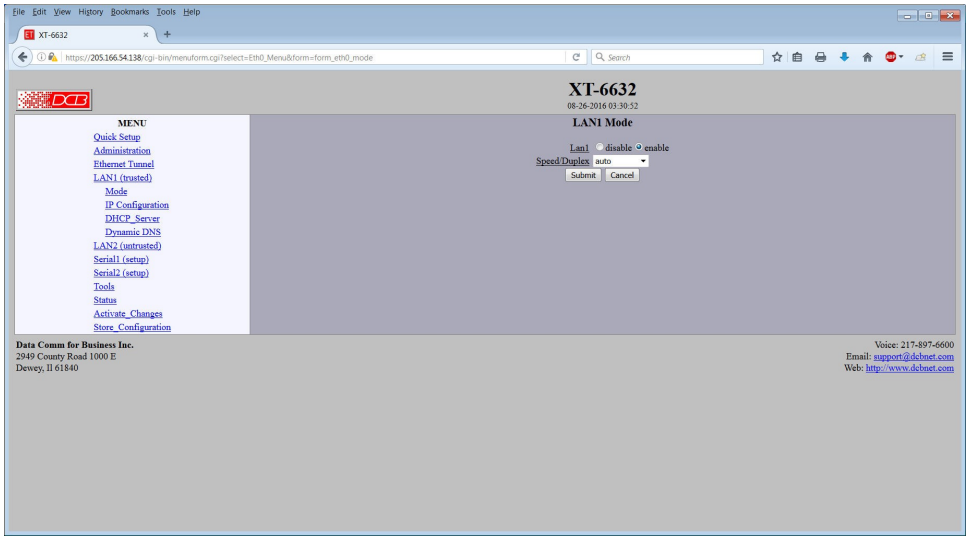
Version Information Screen



Version Information Screen

This screen displays current firmware and hardware version information as well as some copyright notices.

LAN1 Interface Mode



LAN Interface Mode Screen

The XT contains multiple Ethernet interfaces.

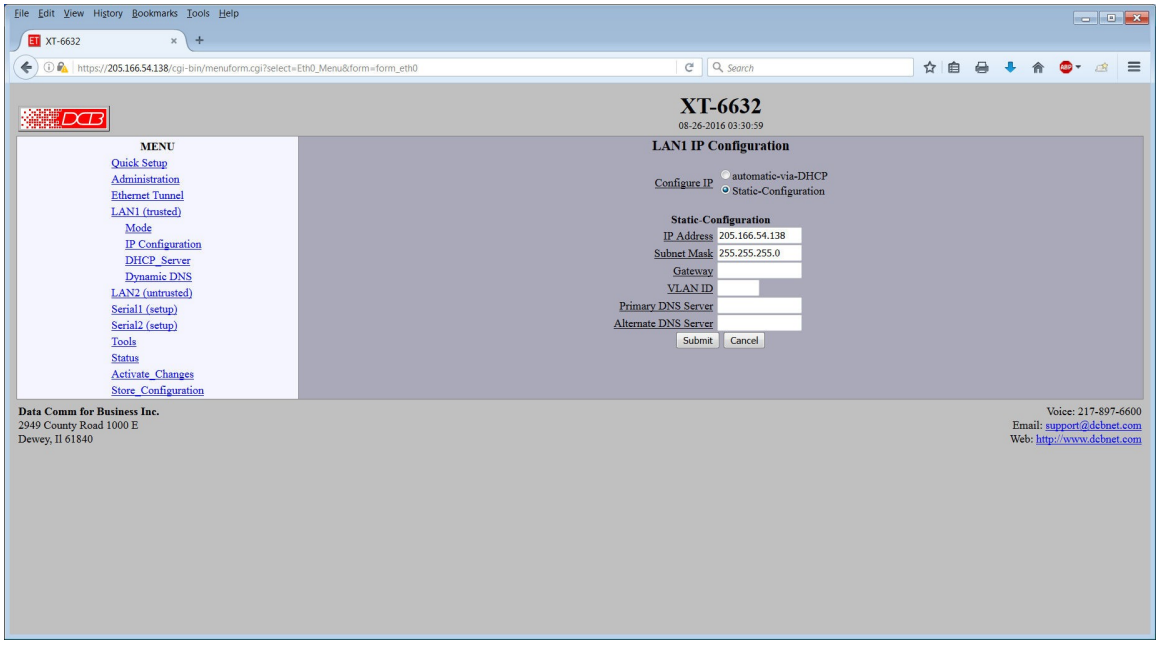
The Ethernet Mode screen is used to select the mode for each ethernet port The Mode screen for LAN1 is limited to enabling the port, and selecting the port speed. Other interfaces are capable of PPPoE, and their mode screen contains additional information. See the Ethernet PPPoE configuration screen section for information pertaining to PPPoE.

Fields

- Enable / Disable
  This should always be set to enable if the interface is to be used.
- Speed/Duplex
  Select AUTO, 10 Mbps half duplex, or 100 Mbps half duplex.. Select the appropriate one for this interface. (Note, some models do not contain this field and are auto-negotiating.)
- Mode (Not available on the trusted interface)
  Select IP or PPPoE

Notes:

LAN 1 IP Configuration



LAN 1 IP Configuration Screen

The XT contains multiple Ethernet interfaces. LAN 1 is always a local, secure side of the tunnel. Other interfaces are the insecure side, and are usually used with a broadband WAN or public Internet connection. This screen is used to configure IP parameters for LAN 1.

Fields

- Configure IP
  Select DHCP or a static configuration. If DHCP is selected, the static-configuration is ignored.
- IP Address
  An IP address is a numeric identifier given to an interface. It consists of four 8-bit numbers and is represented in a dotted notation. An example of an IP address is "192.168.0.10". An Ethernet IP address must be unique within your network. If you are directly connected to the Internet, it must globally unique.
  This field is not used if DHCP Client has been enabled. The DHCP server will assign the IP address.
- Subnet Mask
  A subnet mask is a bit mask applied against the IP address. It specifies which portion of the IP address is the subnet identifier and which portion is the host identifier. For example, many subnets have a mask of 255.255.255.0. This means the first 24 bits of the address is the subnet identifier and the last 8 bits is the host identifier.

  This field is not used if DHCP Client has been enabled. The subnet mask will be assigned by the DHCP server.
- Gateway

  The Gateway specifies the address of the gateway router on the local subnet. Packets destined for a host not on the local subnet are forwarded to the gateway router. This is normally left blank.

The bridge uses policy-based routing rules which allow each interface to have a gateway router defined. Routing decisions take into account the source IP address when selecting a gateway. Instances where a source address has not been established, such as when initiating a connection, ping, etc, the tunnel will give priority to Ethernet-B's gateway.

- VLAN ID
  If the Ethernet interface is attached to an 802.1Q trunk, you must specify a VLAN ID number for the interface. The IP address will be then be bound to this VLAN. This will allow you to access the tunnel's web server through the 802.1Q trunk from the specified VLAN. Valid range is 0 - 4095. Leave blank to disable.

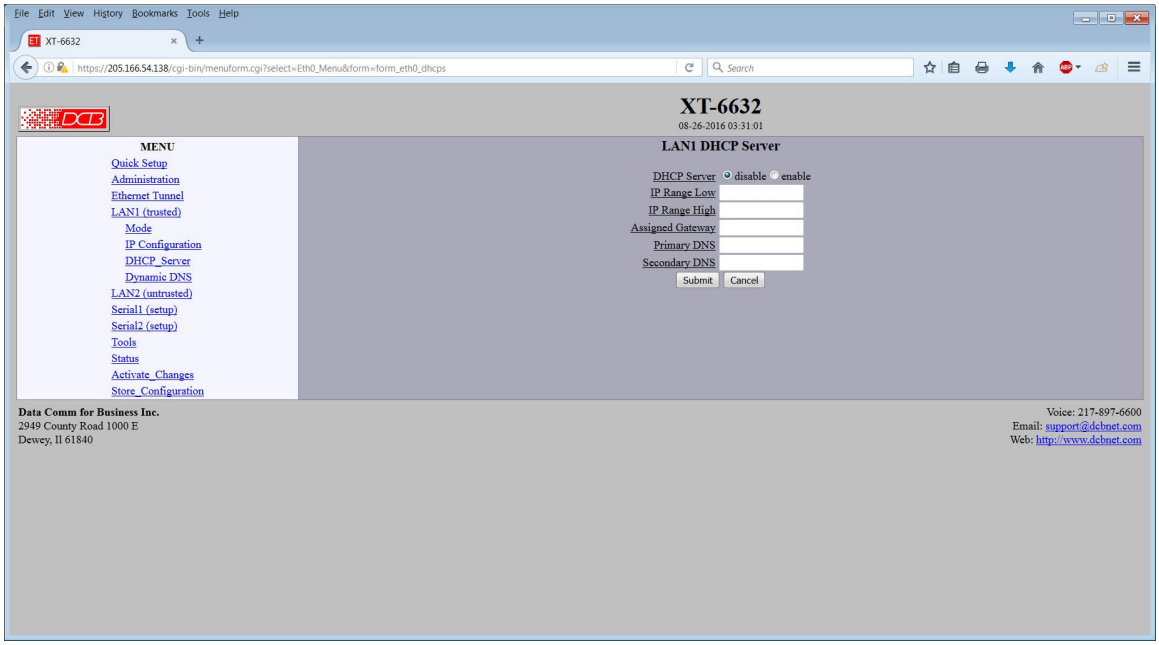
  Note: *Static-configuration* must be used on LAN1 if it is configured for an 802.1Q VLAN.

- Primary DNS
  The IP address of the primary DNS server. This server will be used to resolve host names into ip addresses.

  Note: The DNS servers are common for all interfaces. **If any of the interfaces are configured to use DHCP, the DNS servers assigned by the DHCP server will take precedence.**

- Secondary DNS
  The IP address of the secondary DNS server. This server will be used to resolve host names into ip addresses in the event that the primary name server does not respond or is unable to resolve a name.

LAN 1 DHCP Server Configuration



LAN 1 DHCP Configuration Screen

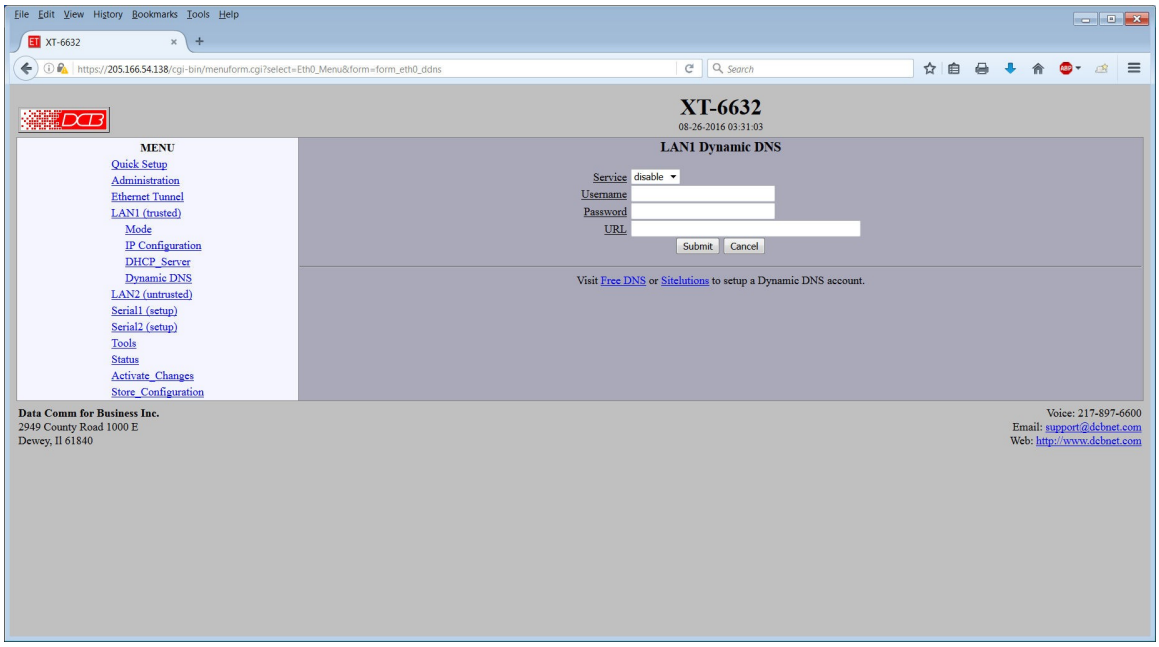
The XT may be configured as a DHCP server to provide IP addresses, Gateway, and DNS server addressing for clients on the local LAN. This screen is used to enable and configure that service.

Fields

- **DHCP Server**
  Enable/Disable a DHCP Server on the interface. Addresses will be dynamically assigned from the following pool in response to DHCP Client requests.
- **IP Address Range Low Value**
  IP Range Low and IP Range High define an inclusive range of IP addresses to administer. The tunnel will dynamically assign these addresses to DHCP clients as requests are received. These addresses must be valid for the interface's subnet. For example, if the interface has an IP address of 192.168.0.1 and a netmask of 255.255.255.0, then the range of IP addresses must be on the 192.168.0 subnet.
- **IP Address Range High Value**
  IP Range Low and IP Range High define an inclusive range of IP addresses to administer. The tunnel will dynamically assign these addresses to DHCP clients as requests are received. These addresses must be valid for the interface's subnet. For example, if the interface has an IP address of 192.168.0.1 and a netmask of 255.255.255.0, then the range of IP addresses must be on the 192.168.0 subnet.
- **Default Gateway**
  This is the default gateway address to be given to the DHCP client. Typically, it would be the IP address of the gateway router on the subnet.
- **Primary DNS**
  This is the primary DNS server address assigned to the DHCP client.

- **Secondary DNS**
  This is the secondary DNS server address assigned to the DHCP client.

LAN 1 Dynamic DNS Configuration



LAN 1 Dynamic DNS Configuration Screen

A Dynamic DNS service allows you to associate a dynamically assigned IP address to a host name and domain. This is achieved by having the device contact the Dynamic DNS service after it has been assigned an IP address. By contacting the Dynamic DNS service, the service is able to detect the device's IP address and will create DNS record for that device.

In order to use Dynamic DNS, you must first setup an account with a Dynamic DNS service provider. We have tested with the service provided by FreeDNS and Sitelutions. However, any URL based service using HTTP Get should work.

The unit will perform a HTTP Get each time an interface is enabled and/or each time the IP address changes.

Fields

- **Service**
  Enable/Disable Dynamic DNS support for the associated interface.
- **Username**
  Optional username for Dynamic DNS servers that require HTTP basic authentication.
- **Passsword**
  Optional password for Dynamic DNS servers that require HTTP basic authentication.
- **URL**
  HTTP url to access when the associated interface is enabled. The url must be in the form of:
  http://www.somewebsite.com/subdirectory?optionalparms
  If the service uses a port number other than 80, you may append the port number following the

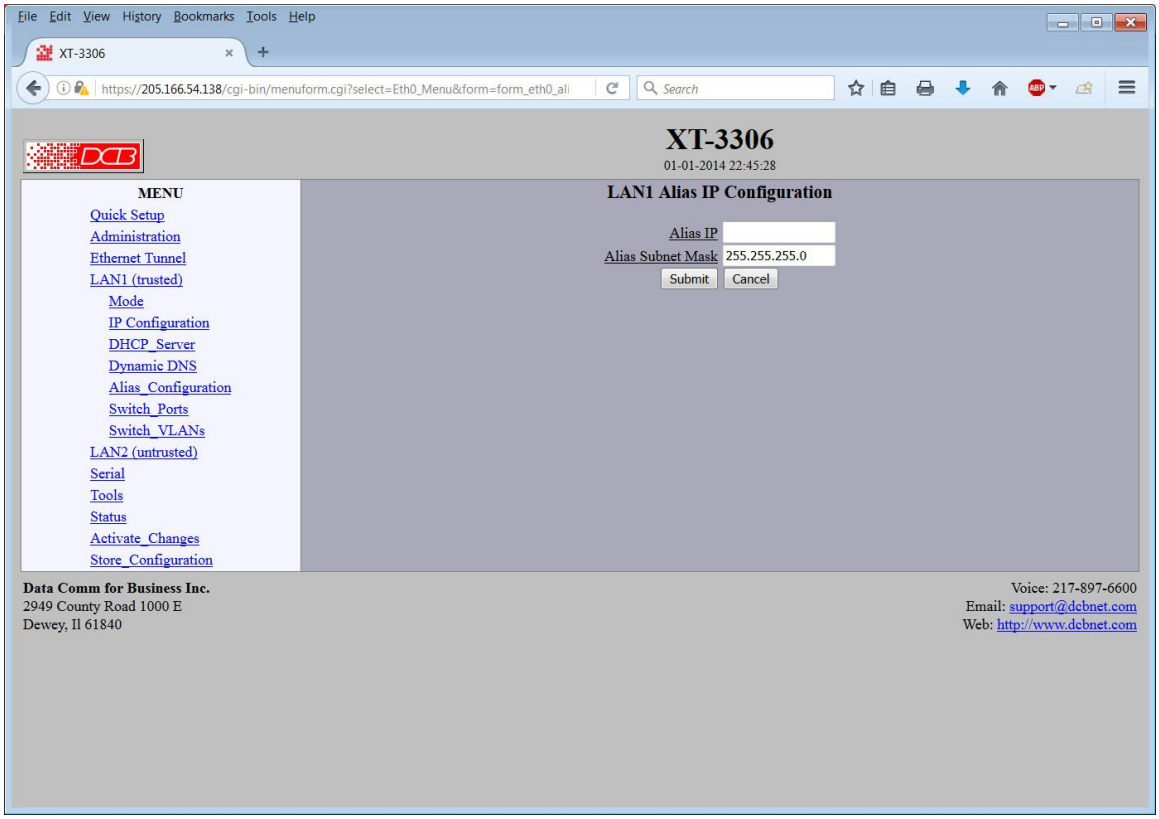
hostname. For example:
http://www.somewebsite.com:8000/subdirectory?optionalparms.
If your service requires you to send your IP address in the URL, insert the string **{IP}**, in the position that the IP address is required. For example:
http://www.somewebsite.com/subdirectory?IP={IP}
Https (SSL) is not supported.

Notes

FreeDNS Configuration Notes:
After creating an account and hostname with FreeDNS simply cut and paste the **Direct_URL** assigned by FreeDNS into the URL field. You do not need to set the username or password fields. The URL should look similar to this:
http://freedns.afraid.org/dynamic/update.php?ABCDEFGabcdefg1234567hijkHIJLlmnopU2

Sitelutions Configuration Notes:
You must first setup an account with Sitelutions then create a DNS record for your host. When you do this, Sitelutions will assign a Dynamic DNS record ID to this entry. The Sitelutions URL to update your DNS record has your email account, password, DNS record ID, and IP address appended as paramters. The URL should look similar to this:
http://www.sitelutions.com/dnsup?user=me@email.com&pass=password&id=1234567&ip={IP}

LAN 1 Alias IP Configuration



LAN 1 Alias IP Configuration Screen

Some models allow a second IP address to be assigned to the trusted interface, LAN1, as an alias.

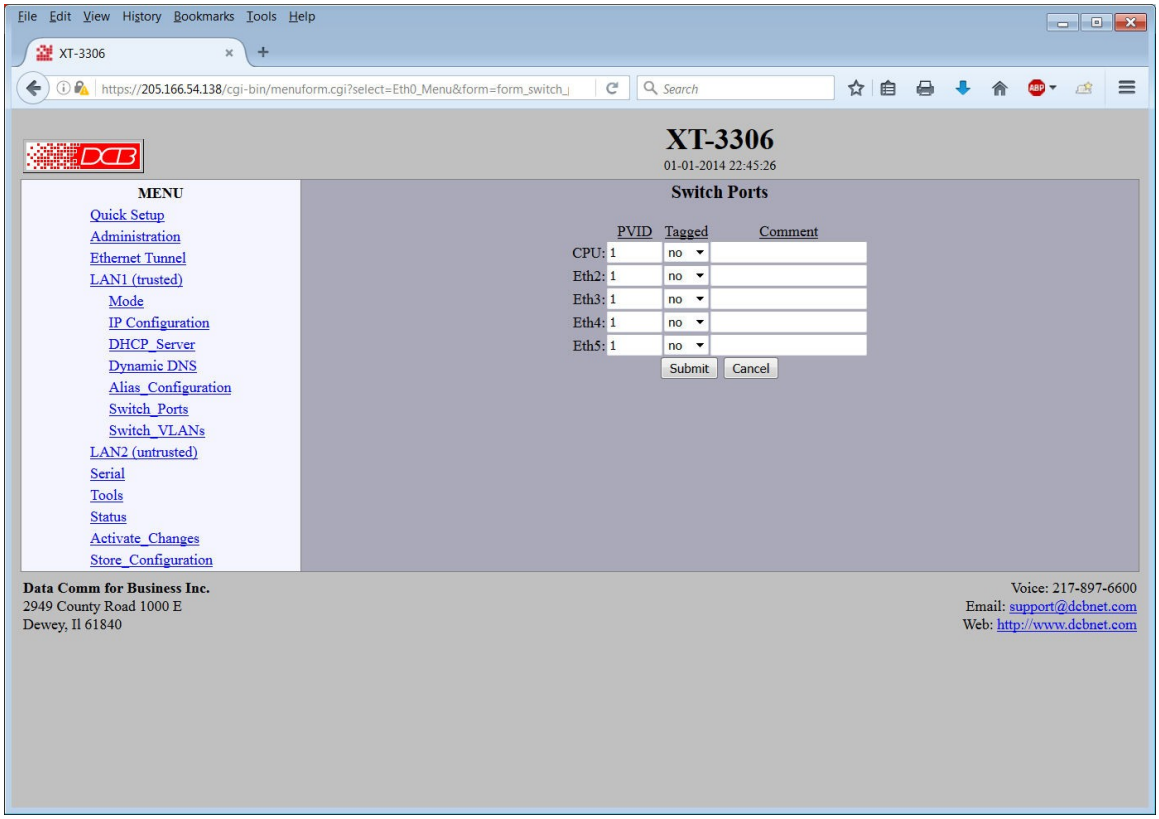
Fields

- **Alias IP**
  An Alias IP address is a secondary IP address given to an interface. This is an optional field.
- **Alias Subnet Mask**
  The subnet mask for the Alias IP Address.

Notes

This feature is rarely used.

XT-3306 Switch Ports Configuration



Switch Ports Configuration Screen

The XT-3306 model contain a four port ethernet switch that supports VLAN. This configuration applies to the integrated Ethernet switch attached to Tunnel's LAN-1 interface. The integrated Ethernet switch is an 802.1Q VLAN aware switch. All Ethernet frames entering the switch will be classified into a VLAN and tagged with a VLAN ID (VID). Ethernet frames exiting the switch may continue to carry the VLAN tag or have the tag removed.

The integrated Ethernet switch has physical ports, Eth2 - Eth6, located on the front of the device. There is also an **internal** port that connects to the Tunnel's LAN-1 interface to the switch. For the purpose of configuration, this internal port is referred to as the **CPU** port. Please use care when configuring your VLANs. **If you accidentally isolate the CPU port from the physical ports, you will lose the ability to manage the device and will have to reset to defaults in order to recover.**

The configuration of the CPU port also controls what traffic the tunnel will carry. All VLANs, in which the CPU is configured as a member, will be carried across the tunnel. If it is carrying tagged traffic, make sure to configure LAN-1 with a VLAN ID for management.

Fields

- **PVID**
  This field sets the default VLAN ID for the port. Untagged Ethernet frames received on the port will

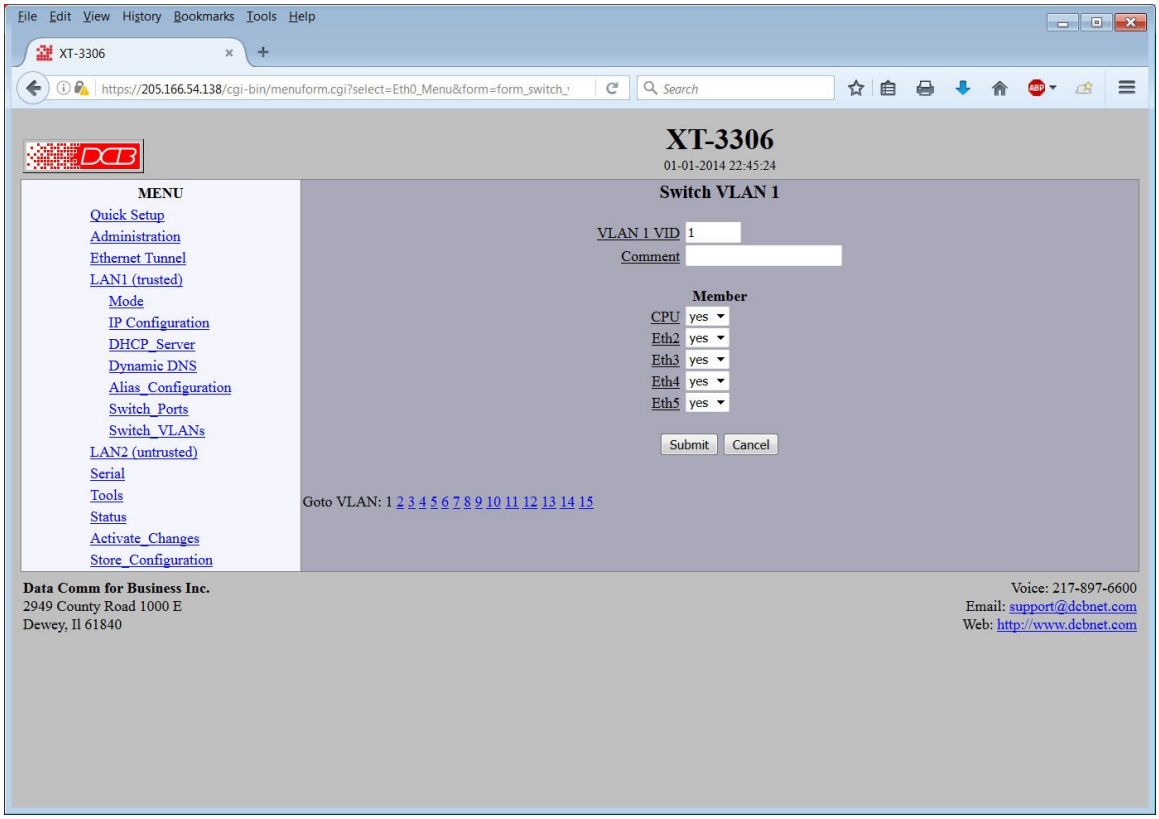
be classified into the VLAN with the matching VID. For example, if the PVID is set to 50, the frame will tagged with a VLAN ID of 50.

- **Tagged**
  This field selects whether or not Ethernet packets will egress the port with a VLAN tag or without a VLAN tag. Please note that unlike some switches, this switch does not support egress of both tagged and untagged packets on the same port.
- **Comment**
  This is a user defined comment field that may be used to document the port usage.

Notes

Use care when configuring VLAN operation as improper configuration can lock out the unit from management requiring a factory reset to recover.

XT-3306 Switch VLAN Configuration



Switch VLAN Configuration Screen

The XT-3306 contain a four port ethernet switch that supports VLAN. This configuration applies to the integrated Ethernet switch attached to Tunnel's LAN-1 interface. The integrated Ethernet switch is an 802.1Q VLAN aware switch. All Ethernet frames entering the switch will be classified into a VLAN and tagged with a VLAN ID (VID). Ethernet frames exiting the switch may continue to carry the VLAN tag or have the tag removed.

This screen is used to configure the individual VLANs on the unit. The XT-3306 is capable of supporting up to 15 VLAN IDs along with the default VLAN 0.

Fields

- **VLAN x VID**
  This field sets the 802.1Q ID number for the VLAN. It may range from 0 - 4094. Please note that VLAN ID 0 is reserved and is used to indicate a frame that does not belong to any VLAN.
- **Comment**
  This is a user defined comment field that may be used to document the port usage.
- **Member**
  These fields select whether or not a port is a member of a VLAN.

  When bridging multiple VLANs across the tunnel connection, make sure the CPU port is a **tagged**

member of each VLAN.

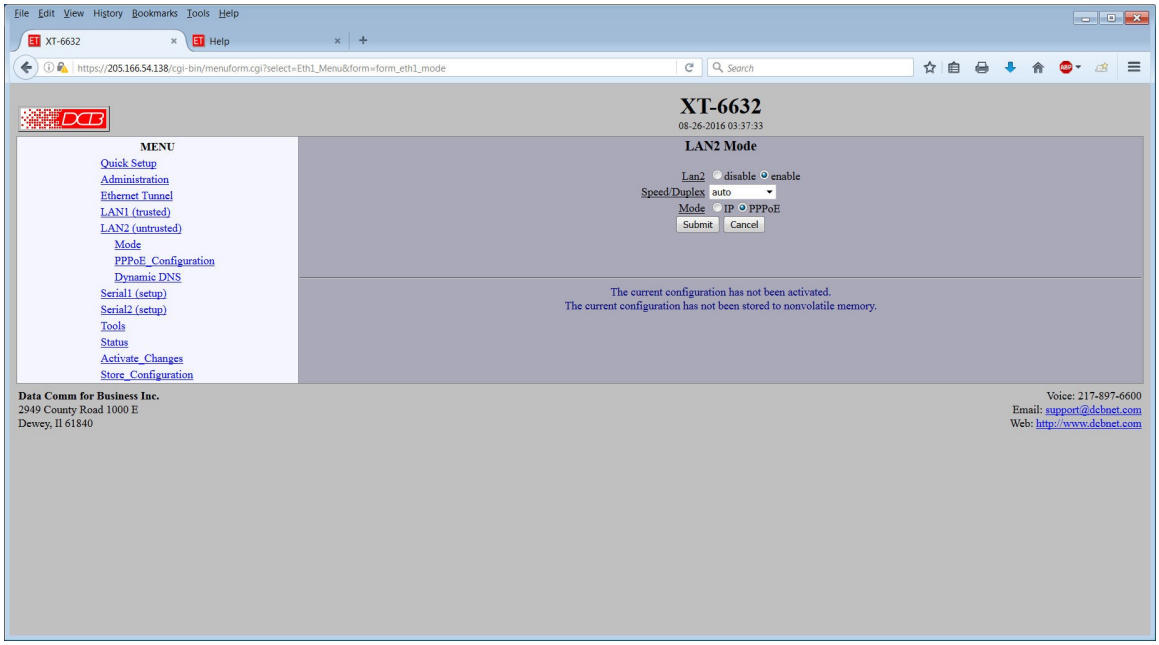
To Isolate a port, give the port a unique PVID and do not make it a member of any VLAN.

- **VLAN**
  Select the VLAN to configure.

Notes

Use care when configuring VLAN operation as improper configuration can lock out the unit from management requreing a factory reset to recover.

LAN 2/3 Mode



LAN 2/3 Mode Screen

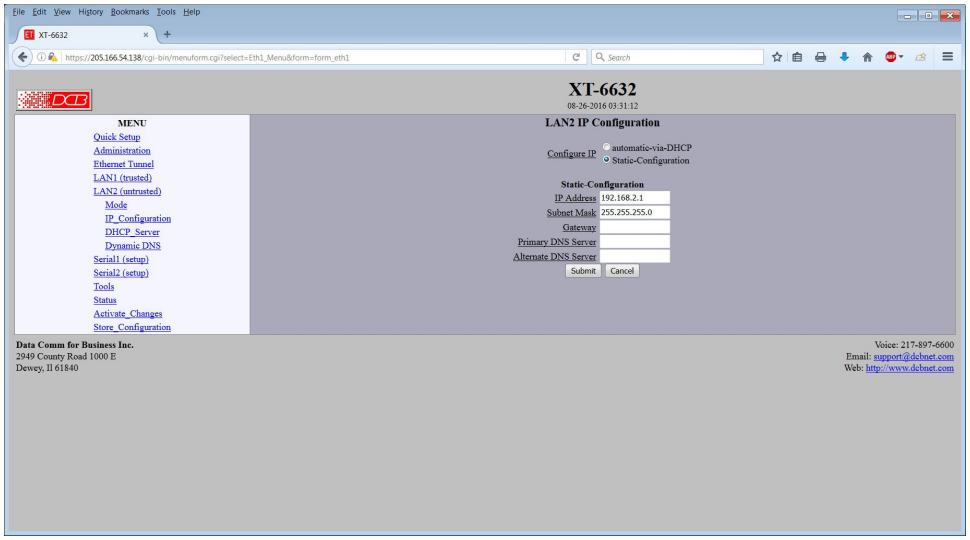
The XT contains multiple Ethernet interfaces. Some models contain a third ethernet interface, LAN3, used as an additional untrusted interface.

The Ethernet Mode screen is used to select the mode for each ethernet port Unlike the LAN1 screen, LAN2 is capable of PPPoE, See the Ethernet PPPoE configuration screen section for information pertaining to PPPoE.

Fields

- Enable / Disable
  This should always be set to enable.
- Speed/Duplex
  Select AUTO, 10 Mbps half duplex, or 100 Mbps half duplex.. Select the appropriate one for this interface.
- Mode
  Select IP or PPPoE. If PPPoE is selected, the Configure PPPoE screen must be configured.

LAN 2/3 IP Configuration



LAN 2 Configuration Screen

The XT contains multiple Ethernet interfaces. The LAN2 interface is used for the “WAN” untrusted connection. LAN 1 is always a local, secure side of the tunnel. The other interface is always the insecure side, and is usually used with a broadband WAN or public Internet connection. This screen is used to configure IP parameters for LAN 2.

Some installations may use PPPOE on this interfaces. On those installations, there is Ethernet Mode screen, used to select the mode for PPPOE. See the Ethernet PPPOE configuration screen section for information pertaining to PPPOE.

Fields

- Configure IP
  Select DHCP or a static configuration. If DHCP is selected, the static-configuration is ignored.
- IP Address
  An IP address is a numeric identifier given to an interface. It consists of four 8-bit numbers and is represented in a dotted notation. An example of an IP address is "192.168.0.10". An Ethernet IP address must be unique within your network. If you are directly connected to the Internet, it must globally unique.
  This field is not used if DHCP Client has been enabled. The DHCP server will assign the IP address.
- Subnet Mask
  A subnet mask is a bit mask applied against the IP address. It specifies which portion of the IP address is the subnet identifier and which portion is the host identifier. For example, many subnets have a mask of 255.255.255.0. This means the first 24 bits of the address is the subnet identifier and the last 8 bits is the host identifier.

  This field is not used if DHCP Client has been enabled. The subnet mask will be assigned by the DHCP server.
- Gateway

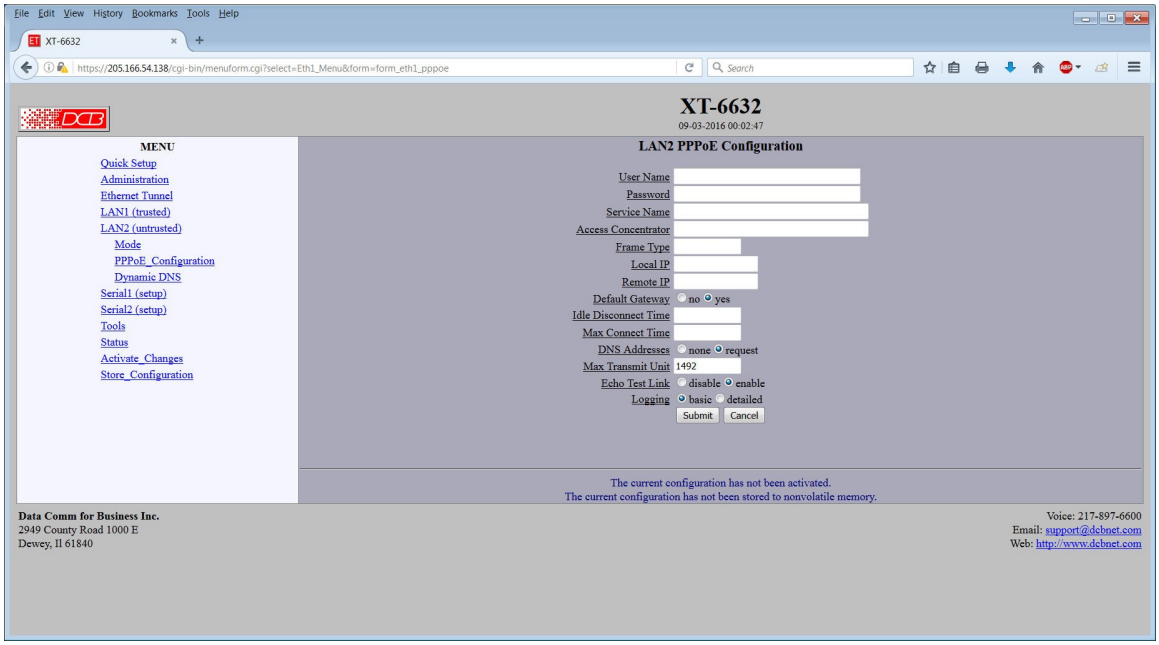
The Gateway specifies the address of the gateway router on the local subnet. Packets destined for a host not on the local subnet are forwarded to the gateway router.

The tunnel uses policy-based routing rules which allow each interface to have a gateway router defined. Routing decisions take into account the source IP address when selecting a gateway. Instances where a source address has not been established, such as when initiating a connection, ping, etc, the tunnel will give priority to LAN2's gateway.

- DHCP Server Settings
  If this unit is to be a DHCP server, the low and high limits for assigned addresses and default gateway must be entered in this section.
- Primary DNS
  The IP address of the primary DNS server. This server will be used to resolve host names into IP addresses.

  Note: The DNS servers are common for all interfaces. If any of the interfaces are configured to use DHCP, the DNS servers assigned by the DHCP server will take precedence.
- Secondary DNS
  The IP address of the secondary DNS server. This server will be used to resolve host names into IP addresses in the event that the primary name server does not respond or is unable to resolve a name.

LAN 2/3 PPPoE Configuration



PPPoE Configuration Screen

PPPoE is available on the LAN 2 and LAN 3 interfaces. This screen is only available for those interfaces that have the mode configured to PPPoE.

Fields

- User name
  This is the user-name to use when authenticating to a PPPoE Server. In other words, this is the user-name sent to the remote server. The user-name may be a string of 1 to 39 printable characters. No space or control characters.
- Password
  This is the password to use when authenticating to a PPPoE Server. In other words, this is the password sent to the remote server. The password may be a string of 1 to 39 printable characters. No space or control characters.
- Service name
  This is an optional field that specifies the desired service name. If set, PPPoE will only initiate sessions with access concentrators which can provide the specified service. Only set this field if instructed to by your ISP.
- Access Concentrator
  This is an optional field that specifies the name of the desired access concentrator. If set, PPPoE will only initiate sessions with the named access concentrator. Only set this field if instructed to by your ISP.
- Frame Type
  This is an optional field that sets the Ethernet frame type for PPPoE discovery and session frames. This field is only used if your ISP uses non-standard PPPoE frame types. The frame types are specified as

hexadecimal numbers separated by a colon. For example: 8863:8864. Only set this field if instructed to by your ISP.

- Local IP
  Each side of a PPP connection will have an IP address. This is the IP address to use for the local PPP device. With PPPoE, you will normally leave this field blank. The PPPoE server will automatically assign an IP address upon connection.

  If you leave this field blank when connecting on-demand, the XT will temporarily assign a local address to the PPPoE interface until actual PPPoE connection is brought up.

- Remote IP
  Each side of a PPP connection will have an IP address. This is the IP address to assign to the remote PPP device. With PPPoE, you will normally leave this field blank. The PPPoE server will report the IP address upon connection.

- Idle Disconnect Time
  Setting an *Idle Disconnect Time* will enable connecting on-demand. The PPPoE connection will come up where there is IP traffic to route out the PPP link and will terminate when the link is idle for the specified amount of time (in minutes).

  This feature is typically used when your ISP charges for service based on connect time.

- Max Connect Time
  Setting *Max Connect Time* will cause the PPPoE connection to terminate when the time limit has been reached, regardless of activity. The time is set in minutes.

  This feature is normally not needed and only used as a workaround for various ISP problems.

- DNS Address
  When set to *request*, the local XT will request DNS addresses from the PPPoE Server during PPP option negotiation. When set to *none*, the local XT will not request DNS addresses, and will use the static DNS configuration.

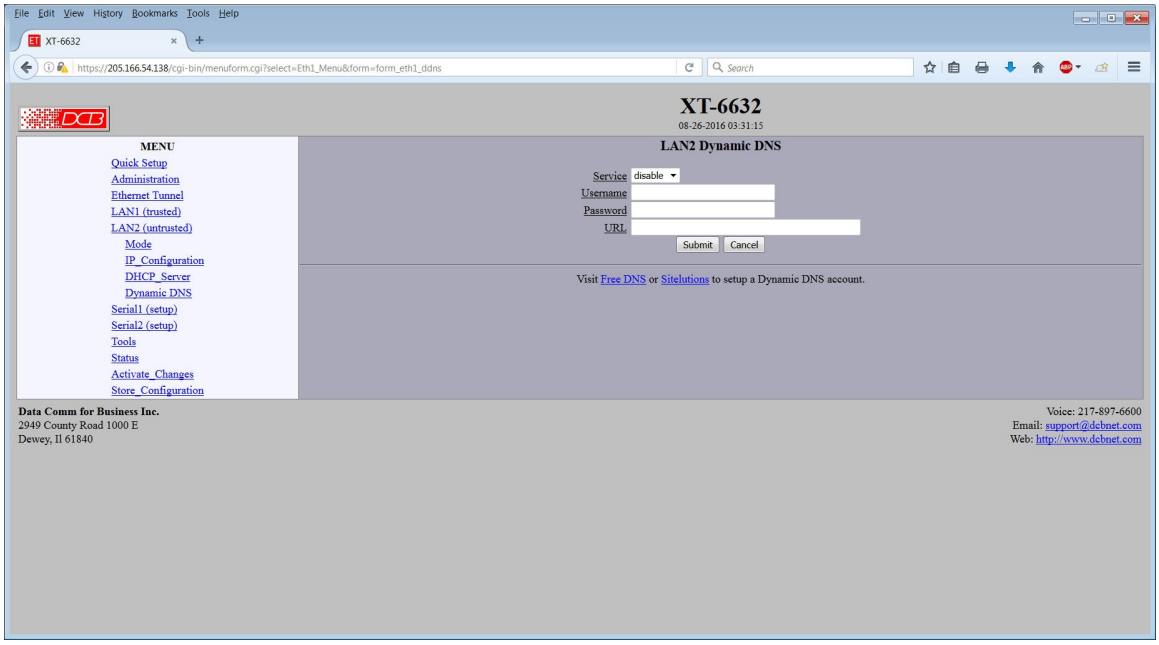
- MTU
  This selects the maximum transmit unit and maximum receive unit for the PPPoE interface. Outgoing network packets will be limited to the specified size. The peer will be asked to limit its MTU to this size. The peer may negotiate a smaller size. The value may be between 128 to 1500. For PPPoE, the recommended setting is 1492.

- Echo Test Link
  When enabled, an LCP level echo request will be sent periodically (30 seconds) to the PPPoE Server. If the server fails to respond to 4 consecutive requests (2 minutes), the link will be taken down and reestablished.

- Logging
  This selects the level of information placed in the PPP log file.

Notes:

LAN 2/3 Dynamic DNS Configuration



LAN 2 Dynamic DNS Configuration Screen

A Dynamic DNS service allows you to associate a dynamically assigned IP address to a host name and domain. This is achieved by having the device contact the Dynamic DNS service after it has been assigned an IP address. By contacting the Dynamic DNS service, the service is able to detect the device's IP address and will create DNS record for that device.

In order to use Dynamic DNS, you must first setup an account with a Dynamic DNS service provider. We have tested with the service provided by FreeDNS and Sitelutions. However, any URL based service using HTTP Get should work.

The unit will perform a HTTP Get each time an interface is enabled and/or each time the IP address changes.

Fields

- **Service**
  Enable/Disable Dynamic DNS support for the associated interface.
- **Username**
  Optional username for Dynamic DNS servers that require HTTP basic authentication.
- **Passsword**
  Optional password for Dynamic DNS servers that require HTTP basic authentication.
- **URL**
  HTTP url to access when the associated interface is enabled. The url must be in the form of:
  http://www.somewebsite.com/subdirectory?optionalparms
  If the service uses a port number other than 80, you may append the port number following the hostname. For example:
  http://www.somewebsite.com:8000/subdirectory?optionalparms.
  If your service requires you to send your IP address in the URL, insert the string **{IP}**, in the position that the IP address is required. For example:

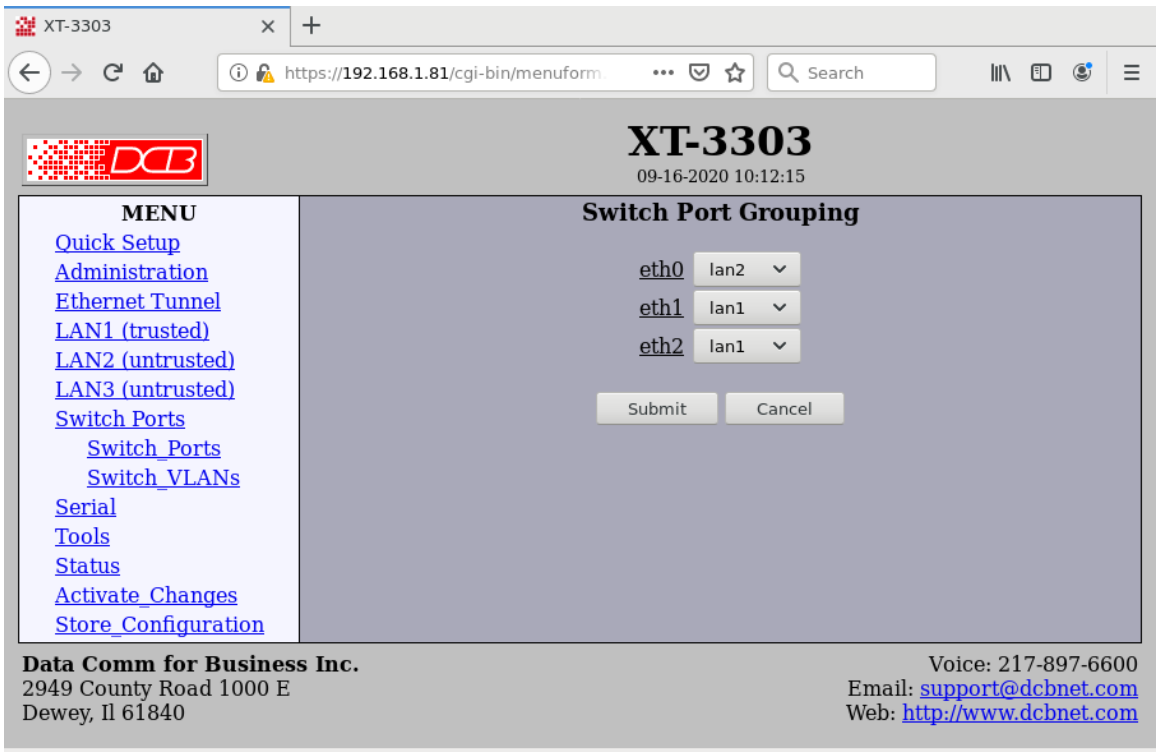
http://www.somewebsite.com/subdirectory?IP={IP}
Https (SSL) is not supported.

Notes

FreeDNS Configuration Notes:
After creating an account and hostname with FreeDNS simply cut and paste the **Direct_URL** assigned by FreeDNS into the URL field. You do not need to set the username or password fields. The URL should look similar to this:
http://freedns.afraid.org/dynamic/update.php?ABCDEFGabcdefg1234567hijkHIJLlmnopU2

Sitelutions Configuration Notes:
You must first setup an account with Sitelutions then create a DNS record for your host. When you do this, Sitelutions will assign a Dynamic DNS record ID to this entry. The Sitelutions URL to update your DNS record has your email account, password, DNS record ID, and IP address appended as paramters. The URL should look similar to this:
http://www.sitelutions.com/dnsup?user=me@email.com&pass=password&id=1234567&ip={IP}

XT-3303 Switch Port Grouping & POE



Switch Port Grouping

The XT-3303 has 3 “soft” ethernet ports. Each physical port **eth0 - eth2** may be assigned to the LAN1 (trusted) network, the LAN2 (untrusted) network, the LAN3 (untrusted) network, or isolated from all traffic. Due to the PoE features of eth0 , this flexibility allows the physical ports to be allocated to the network where this feature can best be utilized. Also, if operating in a mode where LAN2 and LAN3 is not needed, all physical ports may be assigned to LAN1.

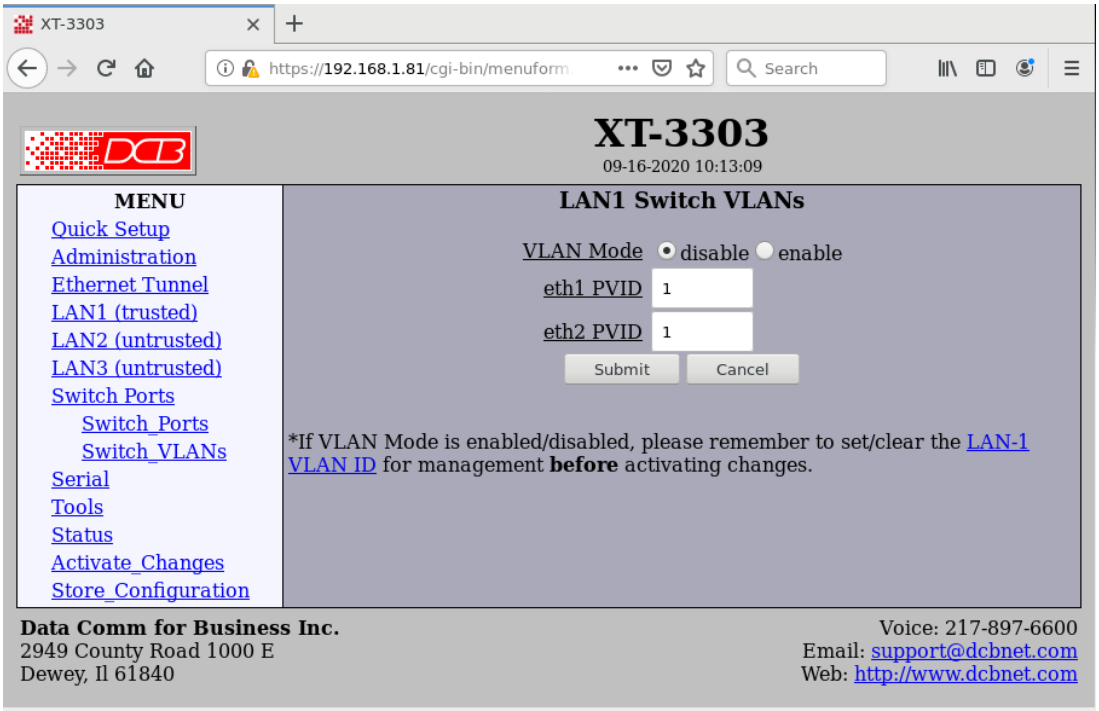
Fields

- **Eth0**
  Eth0 network assignment. This port can receive *passive* PoE.
- **Eth1 - Eth2**
  Network assignments. These ports are not available for PoE

Notes

Powering the XT-3303 with PoE requires 11 to 30VDC at 5 watts. For long cable runs a minimum of 18VDC is recommended to compensate for power loss.

XT-3303 Switch Port VLANs



Switch Port VLAN Screen

This configuration applies to the physical ports assigned to LAN1. In normal operation, the LAN1 switch operates as a basic Ethernet switch, transparently passing Ethernet frames between ports and also across the tunnel connection. However, the switch can also operate in 802.1Q VLAN mode. In this mode, each port is assigned to a VLAN. Ethernet frames received on a port will have an 802.1Q VLAN tag added to the frame. Out-bound frames must have a matching VLAN tag and the VLAN tag will be removed on output. This allows the individual Ethernet ports to be segregated into VLAN groups that extend across the tunnel connection.

Use of the feature requires that the peer tunnel device likewise operate in 802.1Q mode or that the peer tunnel device has an external 802.1Q switch connected to the trusted port.

Before activating this feature, make sure to also configure LAN-1 with a VLAN ID, assigning it to one of your VLANs. This is the VLAN from which you will manage the tunnel device.

Fields

- **VLAN Mode**
  Enable/Disable 802.1Q VLAN mode. When disabled, the LAN1 switch will operate as a transparent switch with all ports in the same LAN. When enabled, the switch is 802.1Q VLAN aware. Each port will operate in the assigned VLAN and Ethernet frames will be VLAN tagged on input and un-tagged on output. If a port is not assigned to a VLAN, it will function as a VLAN trunk.
- **Eth0 PVID**
  Eth0 port VLAN ID (0 - 4095).
- **Eth1 PVID**
  Eth1 port VLAN ID (0 - 4095).

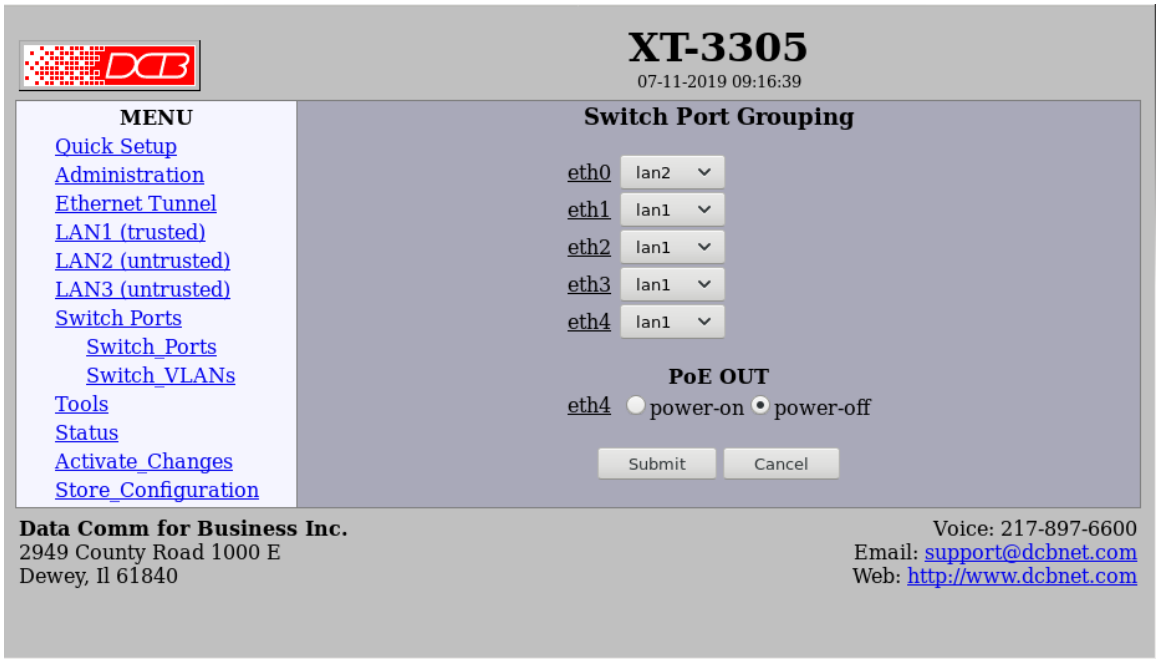
- **Eth2 PVID**
  Eth2 port VLAN ID (0 - 4095).

Notes

Use of the feature requires that the peer tunnel device likewise operate in 802.1Q mode or that the peer tunnel device has an external 802.1Q switch connected to the trusted port.

Before **activating** this feature, make sure to also configure LAN-1 with a VLAN ID, assigning it to one of your VLANs. This is the VLAN from which you will manage the tunnel device.

XT-3305 Switch Port Grouping & POE



Switch Port Grouping & POE Screen

The XT-3305 has five “soft” ethernet ports. Each physical port **eth0 - eth4** may be assigned to the LAN1 (trusted) network, the LAN2 (untrusted) network, the LAN3 (untrusted) network, or isolated from all traffic. Due to the special PoE features of eth0 and eth4, this flexibility allows the physical ports to be allocated to the network where this feature can best be utilized. Also, if operating in a mode where LAN2 and LAN3 is not needed, all physical ports may be assigned to LAN1.

Eth4 has the capability to provide power to other passive PoE devices.

Fields

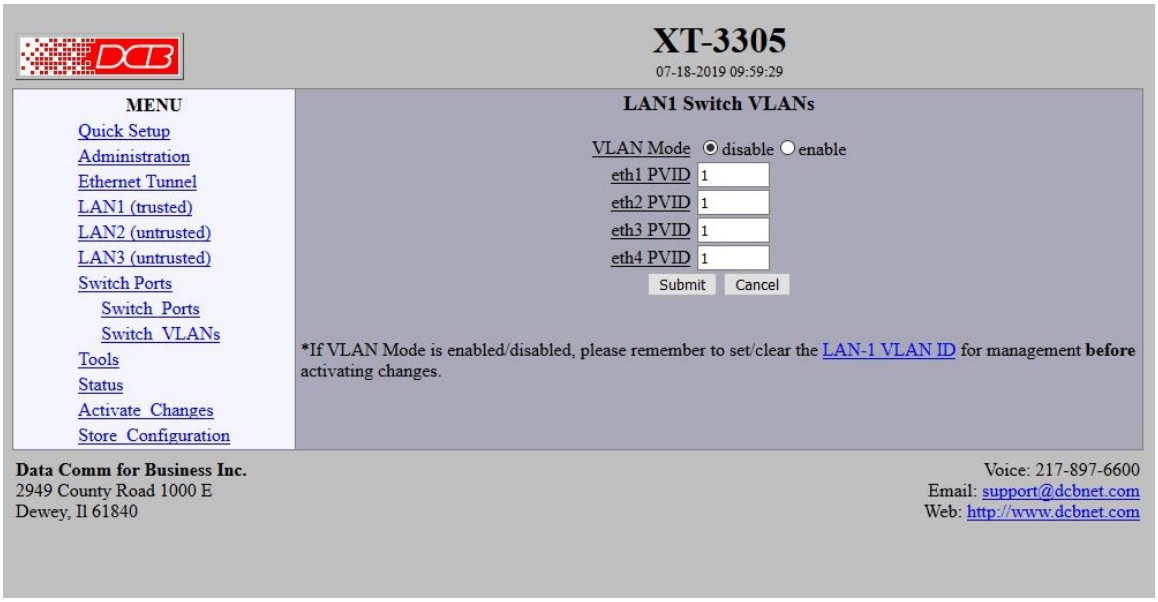
- **Eth0**
  Eth0 network assignment. This port can receive *passive* PoE.
- **Eth1 - Eth3**
  Network assignments. These ports are not available for PoE
- **Eth4**
  Eth4 network assignment. This port can can supply passive PoE
- **Eth4 PoE**
  Enable/disable *passive* PoE power output on eth4. When using this feature, make sure the input power supplied to the tunnel is sufficient to power both the tunnel and the connected device. The tunnel requires 5W of power plus any power used by a connected PoE device. A minimum of 24VDC is recommended when supplying power.

Notes

Powering the XT-3305 with PoE requires 5 watts available from the PoE source at a minimum of 24 volts.

If powering other devices with PoE supplied by the XT-3305, insure that the power supply is capable of supplying the 5 watts required for the XT as well as additional power for the external PoE device.

XT-3305 Switch Port VLANs



Switch Port VLAN Screen

This configuration applies to the physical ports assigned to LAN1. In normal operation, the LAN1 switch operates as a basic Ethernet switch, transparently passing Ethernet frames between ports and also across the tunnel connection. However, the switch can also operate in 802.1Q VLAN mode. In this mode, each port is assigned to a VLAN. Ethernet frames received on a port will have an 802.1Q VLAN tag added to the frame. Out-bound frames must have a matching VLAN tag and the VLAN tag will be removed on output. This allows the individual Ethernet ports to be segregated into VLAN groups that extend across the tunnel connection.

Use of the feature requires that the peer tunnel device likewise operate in 802.1Q mode or that the peer tunnel device has an external 802.1Q switch connected to the trusted port.

Before activating this feature, make sure to also configure LAN-1 with a VLAN ID, assigning it to one of your VLANs. This is the VLAN from which you will manage the tunnel device.

Fields

- **VLAN Mode**
  Enable/Disable 802.1Q VLAN mode. When disabled, the LAN1 switch will operate as a transparent switch with all ports in the same LAN. When enabled, the switch is 802.1Q VLAN aware. Each port will operate in the assigned VLAN and Ethernet frames will be VLAN tagged on input and un-tagged on output. If a port is not assigned to a VLAN, it will function as a VLAN trunk.
- **Eth0 PVID**
  Eth0 port VLAN ID (0 - 4095).
- **Eth1 PVID**
  Eth1 port VLAN ID (0 - 4095).
- **Eth2 PVID**
  Eth2 port VLAN ID (0 - 4095).

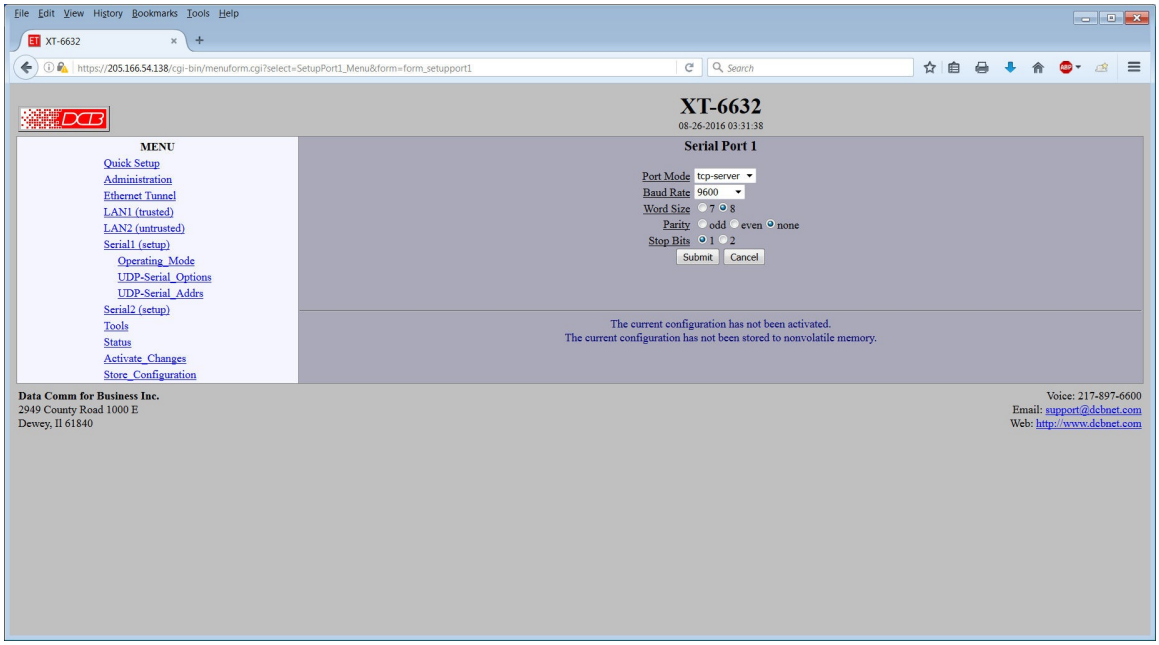
- **Eth3 PVID**
  Eth3 port VLAN ID (0 - 4095).
- **Eth4 PVID**
  Eth4 port VLAN ID (0 - 4095).

Notes

Use of the feature requires that the peer tunnel device likewise operate in 802.1Q mode or that the peer tunnel device has an external 802.1Q switch connected to the trusted port.

Before **activating** this feature, make sure to also configure LAN-1 with a VLAN ID, assigning it to one of your VLANs. This is the VLAN from which you will manage the tunnel device.

Serial 1 Operating Mode



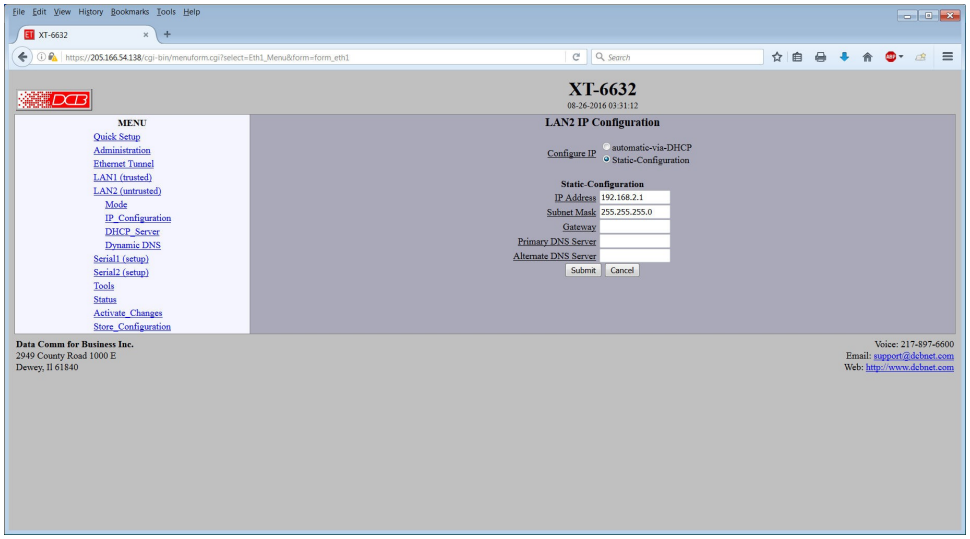
Serial 1 Operating Mode Screen

Some XT products support an RS-232 serial port. The port may be configured to be disabled, a setup port, or a TCP/IP or UDP/IP serial server.

Fields

- Mode
  Sets the operating mode of the port or disables it completely.
- Baud Rate
  Serial port Baud rate.
- Word Size
  Number of data bits in each character. Ignored in setup mode.
- Parity
  Enable parity generation and testing. Ignored in setup mode.
- Stop Bits
  Select between 1 or 2 stop bits. Ignored in setup mode.

UDP Serial Options



UDP Serial Options Screen

When the serial port mode is set to UDP Server", the serial port has features similar to the DCB EtherPoll UDP serial server.

Fields

- **Timer Mode**
  This field selects the method in which serial input data is pushed to the network. In *Transmit-Timer* mode, data is pushed out at a periodic rate. In *Idle-Timeout* mode, data is pushed out when no new data arrives.

- **Transmit Time**r
  When Timer Mode is set to *Transmit-Timer*, this is the time between transmit bursts. When Timer Mode is set to *Idle-Timeout*, any buffered data will be transmitted if no new data arrives within this period. Valid range is 5ms to 10,000ms. Due to system overhead, the actual time may be greater than the specified value, especially for settings below 20ms.

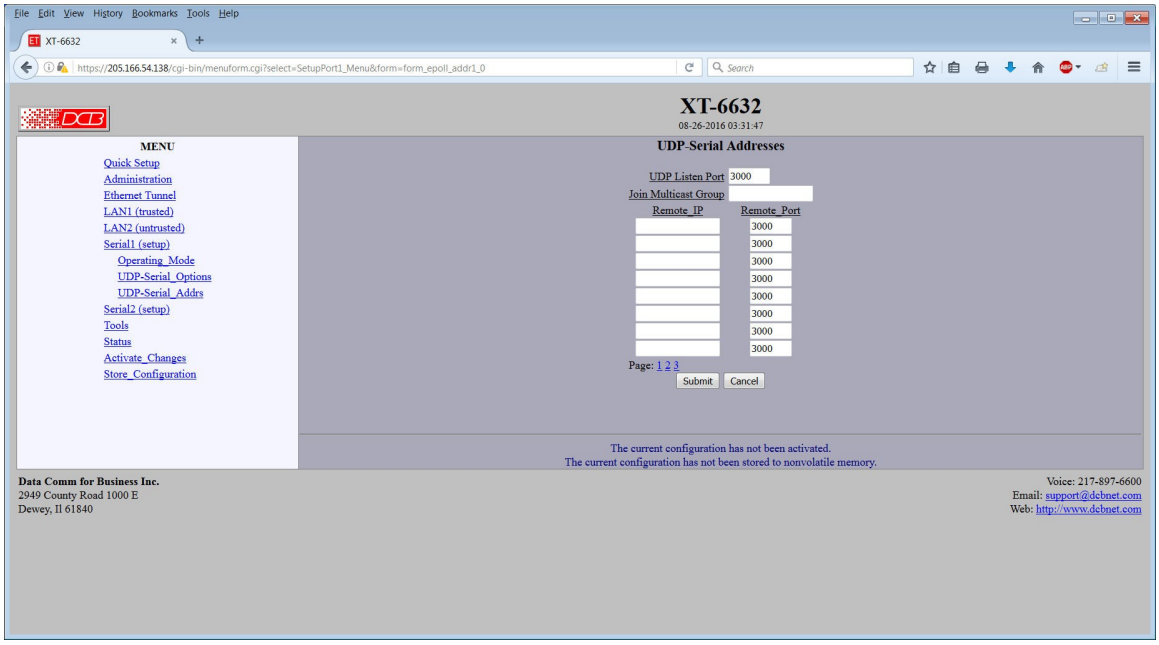
- **Transmit on Block Size**
  This field sets the serial input buffer threshold level. If the number of bytes in the serial input buffer reaches this level, it will push the data to the network, even if the Transmit Timer has not expired.

- **Transmit on Line Termination Character**

  Enable/disable Transmit on Line-Termination character. As serial data is received, it is scanned for a Line-Termination character. If one is detected, it will push the serial data to the network even if the Transmit Timer has not expired.

- **Line Termination Character (0-255)**
  This field sets the Line-Termination Character. It is entered as the decimal value of the character (0 - 255).

UDP Serial Addresses



UDP Serial Addresses Screen

When the serial port mode is set to UDP Server", the serial port has features similar to the DCB EtherPoll UDP serial server. It can receive and "broadcast" incoming packets to up to 30 remote IP addresses.

Fields

- **UDP Listen Port**
  This field specifies the TCP or UDP Port that the unit will listen to for connections or for incoming UDP-Serial datagrams. It also specifies the source UDP port when sending UDP-Serial datagrams. Valid range 1 - 65535.

- **Join Multicast Group**
  This field is optional and will be blank in the normal configuration. If a multicast group is specified, the unit will join the multicast group and receive any datagrams sent to that group. A multicast group is an IP address in the range 224.0.0.0 through 239.255.255.255.

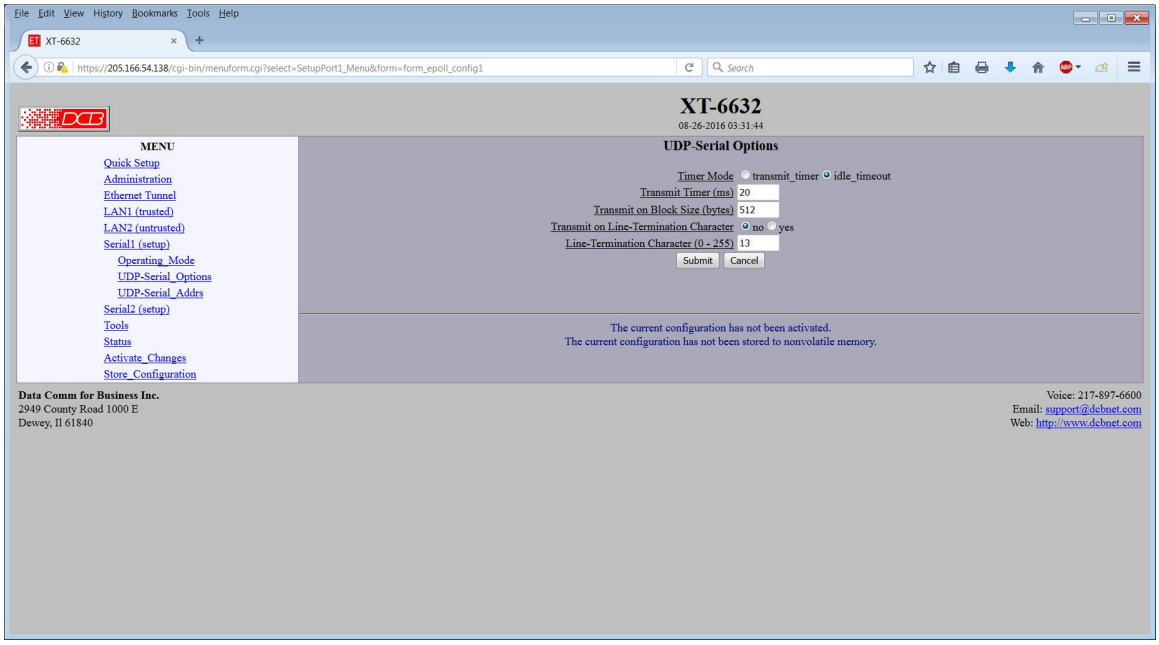
  If this field is blank, the unit will not listen to any multicast groups.

  When choosing a multicast group address make sure to choose one that is not already in use on your network. The range 224.0.0.0 through 224.0.0.255 is typically in use by routers.

- **Remote IP, Remote Port**
  This table specifies the IP address and port number of where UDP-serial datagrams should be sent. The serial input data will be copied and sent to every host in the table. Also, the unit will only accept UDP-serial datagrams from hosts in this table.

  If there are no hosts in this table, the unit will accept datagrams from any host. It will remember the IP address of the last host to send a datagram and will send any incoming serial data back to that same host.

TCP Serial Options



TCP Serial Options Screen

When the serial port mode is set to TCP Server", the serial port has features similar to the DCB EtherPath TCP serial server.

Fields

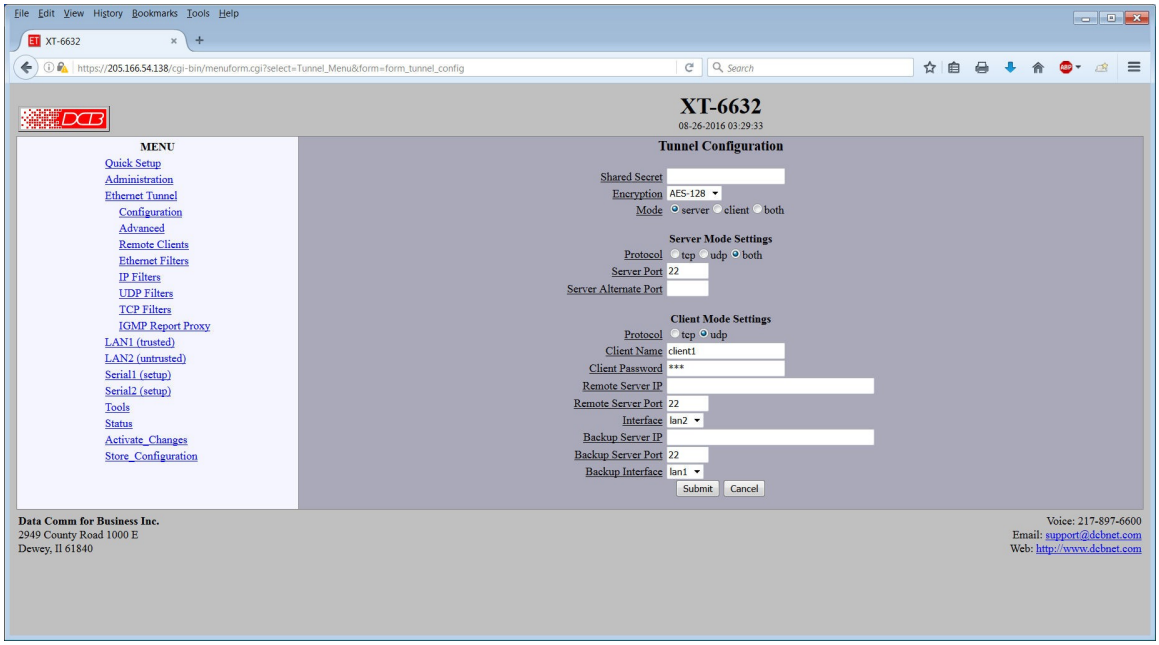
- **TCP Listen Port**
  This field specifies the TCP or UDP Port that the unit will listen to for connections or for incoming UDP-Serial datagrams. It also specifies the source UDP port when sending UDP-Serial datagrams. Valid range 1 - 65535.
- **Server Mode**
  The TCP server can operate in either raw or telnet mode. In raw mode, all data is passed transparently between the serial port and the TCP connection. In telnet mode, telnet command processing will occur and telnet escaping rules will be followed.
- **Idle Disconnect**
  This field sets the time, in minutes, where the TCP connection will be terminated if no data is exchanged with the client. A value of 0 disables the timer.
- **TCP No Delay**
  This option controls Nagle's algorithm. When TCP No-Delay is enabled, Nagle's algorithm is disabled, allowing small packets to be streamed without waiting for the ACK. Enabling TCP No-Delay can have a negative effect on network congestion, but will improve delivery of real-time data.
- **Timer Mode**
  This field selects the method in which serial input data is pushed to the network. In *Transmit-Timer* mode, data is pushed out at a periodic rate. In *Idle-Timeout* mode, data is pushed out when no new data arrives.
- **Transmit Timer**
  When Timer Mode is set to *Transmit-Timer*, this is the time between transmit bursts. When Timer

Mode is set to *Idle-Timeout*, any buffered data will be transmitted if no new data arrives within this period. Valid range is 5ms to 10,000ms. Due to system overhead, the actual time may be greater than the specified value, especially for settings below 20ms.

- **Transmit on Block Size**
  This field sets the serial input buffer threshold level. If the number of bytes in the serial input buffer reaches this level, it will push the data to the network, even if the Transmit Timer has not expired.
- **Transmit on Line Termination Character**

  Enable/disable Transmit on Line-Termination character. As serial data is received, it is scanned for a Line-Termination character. If one is detected, it will push the serial data to the network even if the Transmit Timer has not expired.
- **Line Termination Character (0-255)**
  This field sets the Line-Termination Character. It is entered as the decimal value of the character (0 - 255).

Ethernet Tunnel Configuration



Ethernet Tunnel Configuration Screen

Fields

Shared Secret
The shared secret provides the initial level of privacy. All tunnels participating in the private network must have the same shared secret. This secret phrase is used to generate the AES key used to cypher the initial communications. The secret phrase may be up to 51 characters in length. Do not use a quote or backslash character in the phrase. Best security requires a long, random shared secret.

Encryption
This options selects the encryption method for data passed between the tunnels. Encryption is available in 128 bit, 192 bit, or 256 Bit AES. AES, also known as Rijndael, is a NIST approved encryption method. “None” disables encryption and is used for greatest throughput when encryption security isn't required.

Mode

Server, Client, or Both. Select the mode for this unit. It is permissible for a tunnel to be both a server and client simultaneously.

Server Mode Settings:

Protocol

This option configures the server to operate in TCP mode, UDP mode, or both TCP and UDP mode.

Server Port

The UDP/IP port to listen to when server mode is enabled.

Server Alternate Port

The server may be configured use a second UDP port. This is optional. When used, the client tunnels may be configured to use either server port. The purpose of this option is to allow an alternate connection path

through a router with multiple network up-links. The port number may then be used to differentiate the path.

Client Mode Settings:

Protocol

This option configures the client to operate in TCP mode or UDP mode.

Client Name

This is the client name sent to the server tunnel when authenticating. The server must have a matching name in the table of Authorized Remote Clients. The client name may be up to 51 characters in length. Do not use a quote or backslash character in the phrase.

Client Password

This is the client password used to authenticate the client to the server. The server must have a matching password in its table of Authorized Remote Clients. The password may be up to 51 characters in length. Do not use a quote or backslash character in the phrase.

Remote Server IP

The hostname or IP address of the server tunnel. That is the address this client will connect to.

Remote Server Port

The UDP/IP port to connect to when client mode is enabled. The server must be listening on this port.

Interface

Selects network interface to use when connecting to the server.

Backup Server IP

The IP address or hostname of an alternate server tunnel to connect to in the event that the client is unable to connect to the primary server.

Backup Server Port

The UDP/IP port on the backup server tunnel to connect.

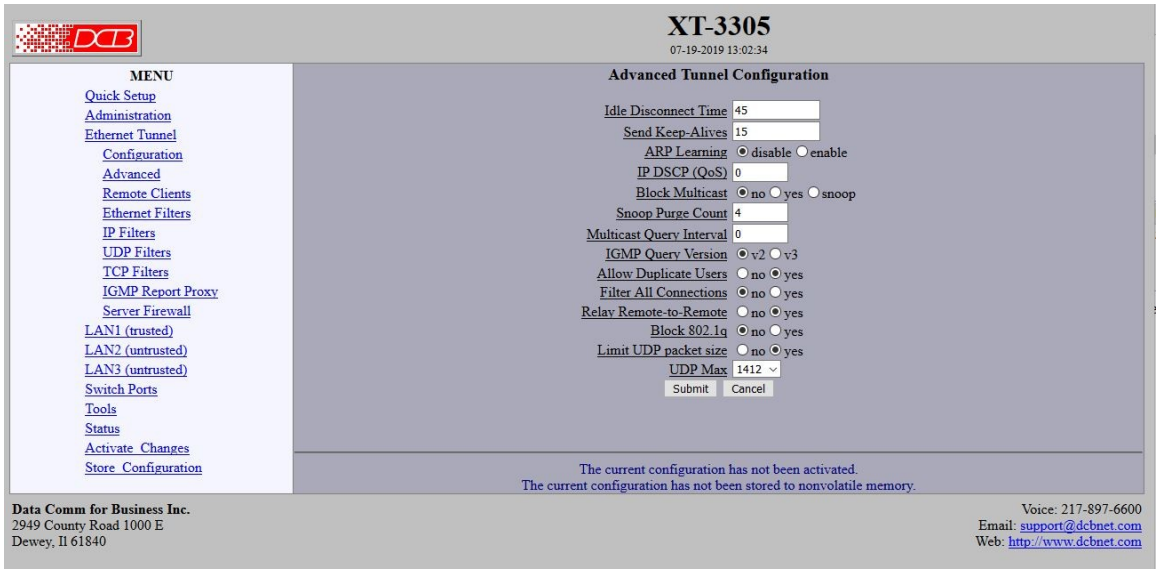
Interface

Selects network interface to use when connecting to the server.

Notes

The XT should never be used in actual applications without changing all passphrases. When used as a non-encrypting bridge, there is no security on the link between the XTs, and all traffic may be monitored by any node in the link, just as with any other bridge or router.

Advanced Tunnel Configuration



Advanced Tunnel Configuration Screen

Fields

Idle Disconnect Time
Setting a time enables an idle disconnect timer. If no packets are received from a remote tunnel for the specified amount of time, the IP connection with that remote tunnel is closed. Time is in seconds. If blank or set to zero, idle disconnect is disabled**.**

Send Keep-Alives
Setting a time enables a keep-alive feature. If the tunnel has not sent anything to the remote tunnel for the specified amount of time, a keep-alive message is sent. This feature is used to prevent an Idle Disconnect. Time is in seconds. If blank or set to zero, keep-alive is disabled.

ARP Learning
Enable/disable ARP learning. When enabled, the tunnel will monitor the Address Resolution Protocol (ARP) to learn the location of IP addresses. It will then use this knowledge to direct ARP broadcasts to a specific location rather than repeating a broadcast to all remote locations.

DSCP (Differentiated Services Codepoint)
This option allows you to set the Differentiated Services Codepoint (DSCP) Field in the IP header of the tunnel's UDP packets. A value of zero select the default behavior. Any value between 0 and 63 is allowed. Interpretation of DSCP and its effect on Quality of Service (QoS) is dependent upon the network infrastructure.

Block Multicast

Setting this option to yes will cause the tunnel to block multicast traffic from being sent to the remote tunnels. Multicast traffic received from remote tunnels will still be output on the local LAN.

Snoop Purge Count

This option only applies when IGMP snooping is enabled. Hosts that do not respond to an IGMP query will eventually be purged from the IGMP snooping table. This option sets the number of missed reports required before purging an entry. The snoop purge count should be 3 or larger.

IGMP Query Version

This option only applies when IGMP snooping is enabled and/or the Multicast Query Interval is non zero. This option sets the version of IGMP to use for query messages. However if a multicast router is detected on the network, the tunnel will mimic the multicast router's IGMP version.

Multicast Query Interval

A value of 0 disables the feature. A non-zero value enables periodic sending of IGMP query messages and sets the IGMP query interval, in seconds. 125 seconds is the typical IGMP query interval.

When the tunnel is performing IGMP snooping, it is reading IGMP reports to determine where multicast traffic should be forwarded. A host computer will send an IGMP report when it wishes to receive (join) or stop receiving (leave) a channel. However, IGMP is an unreliable protocol and it is possible for an IGMP report to be missed. To compensate for this, a multicast router will periodically send an IGMP Query message causing the hosts to report the channels they are receiving. If your network does not have a multicast router, then you should configure the tunnel to send IGMP Query messages.

There should only be one IGMP querier on a network. If your network has a multicast router, you should not enable the Multicast Query Interval in the tunnel. If you need the tunnel to provide backup, in the event the multicast router is down, set the Multicast Query Interval to a time larger than the Query Interval time configured in the router. Most routers default to 125 seconds.

Allow Duplicate Users
This option only applies to the server tunnel. When set to *no*, the server will only allow one instance of a client, based on the client's username, to be connected.

Filter All Connections

Bridge filters (Ethernet, IP, UDP, and TCP) are normally applied only to the packets traveling in from the local Ethernet toward a remote tunnel. If this field is set to *yes*, filters will be also be applied to packets incoming on all tunnel connections.

Important note, setting this feature to yes will eliminate the ability to have a service enabled at one endpoint while blocking that service in the opposite direction. The service is effectively disabled in all directions.

Relay Remote-to-Remote

When set to *yes*, the local tunnel will relay packets between remote tunnels. When set to *no* the local tunnel will only bridge packets to/from the local LAN.

Block 802.1Q Tagged Packets

When set to *yes*, the local tunnel will not relay 802.1Q tagged packets received on the LAN interface to remote tunnels.

Limit UDP Packet Size

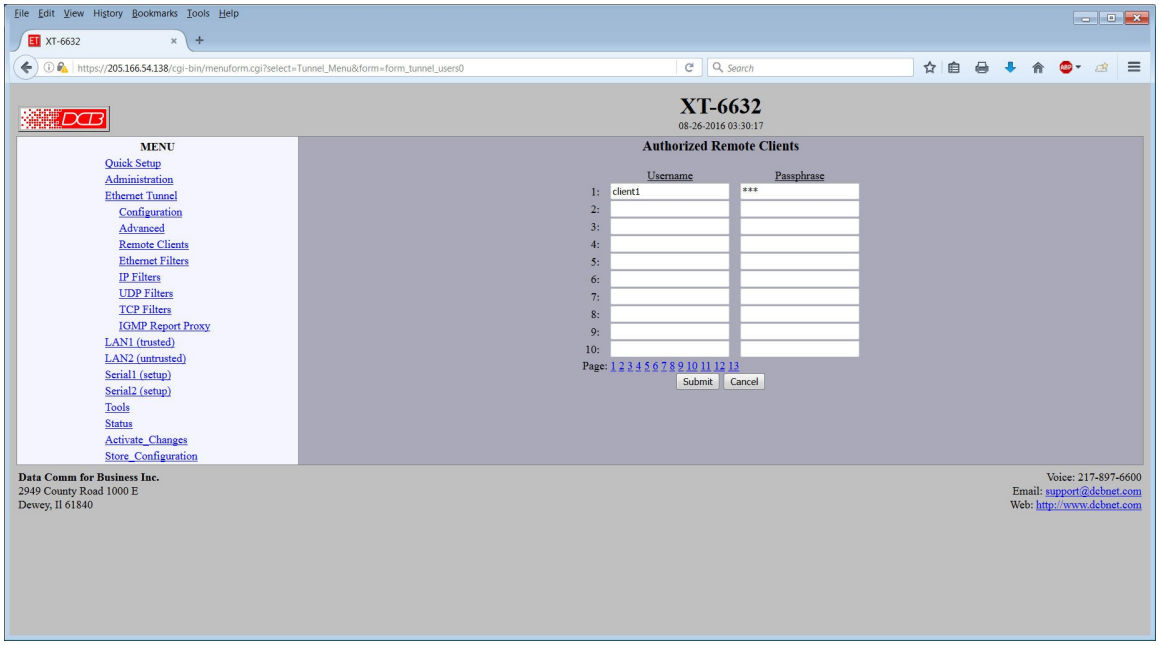
When set to *yes*, the local tunnel will limit the size of UDP packets sent out the untrusted interface to 1412 bytes, not including IP and Ethernet headers. Limiting the packet size will eliminate IP fragmentation on Ethernet networks with a MTU of 1500 bytes. This may be necessary when routing through a firewall that will not pass IP fragments.

UDP Max
This option allows adjustment of the packet size enforced by the Limit UDP Packet Size feature. 1188 bytes is a better choice when tunneling across an LTE network or tunneling inside of another VPN tunnel.

Important Note: This option must be set to 1412 bytes when connecting with older UT/XT devices that do not support the UDP Max feature.

When set to *yes*, the local tunnel will limit the size of UDP packets sent out the untrusted interface to 1412 bytes, not including IP and Ethernet headers.

Remote Clients Screen



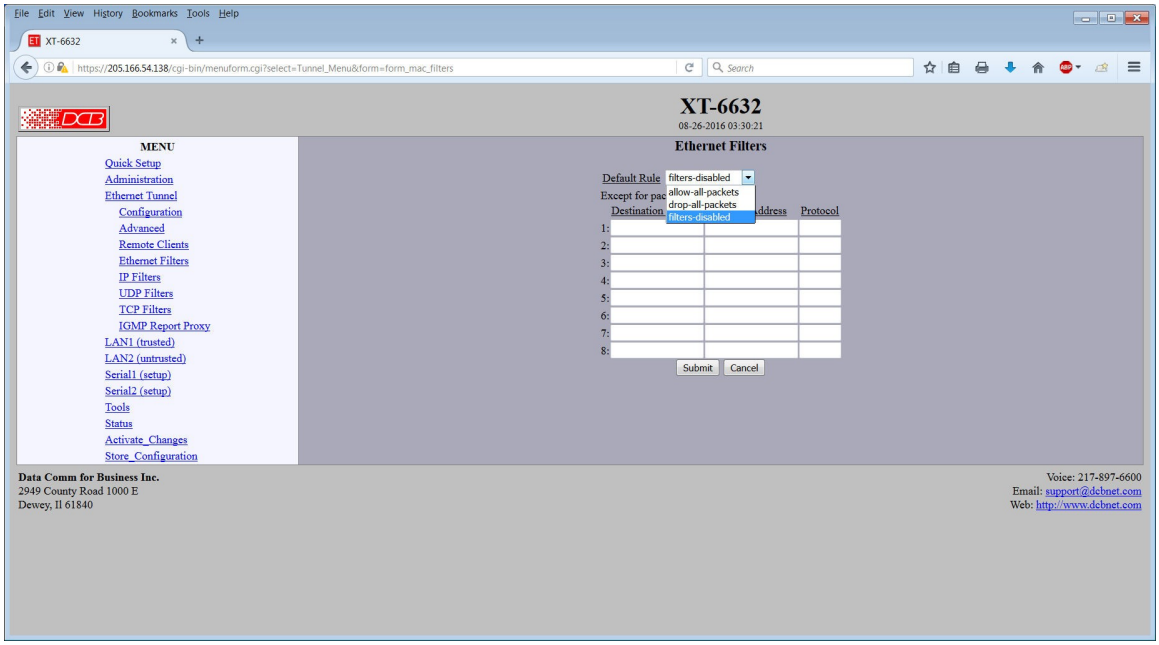
Remote Clients Screen

This table specifies the names and passwords for remote Tunnel clients. It is used by the Server Tunnel to authenticate Client Tunnels. The number of remote clients allowed varies with the specific model.

Fields

- Client Name
  The name may be up to 51 characters in length. Do not use a quote or backslash character in the phrase. If blank, this entry is ignored. .
- Client Password
  AThe password may be up to 51 characters in length. Do not use a quote or backslash character in the phrase. If blank, this entry is ignored.

Ethernet (MAC) Address Filters Screen



Ethernet Address Filters Screen

Ethernet filters are used to limit the Ethernet packets sent from the local tunnel to a remote tunnel. Filtering is performed by comparing the destination address, source address, and protocol ID addresses against a table of rules.

To use Ethernet filtering, you first select a default rule. That is, you choose to **allow all** Ethernet packets by default, or to **drop all** Ethernet packets by default.

Next, you enter one or more exceptions to the default rule. An exception consists of a destination address, source address, and protocol ID. Any packet matching all three items will be considered an exception, causing the opposite of the default rule to be performed.

Please note that Ethernet filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

For Ethernet frames tagged an 802.1Q protocol ID, the protocol ID of the original frame will be used for comparison.

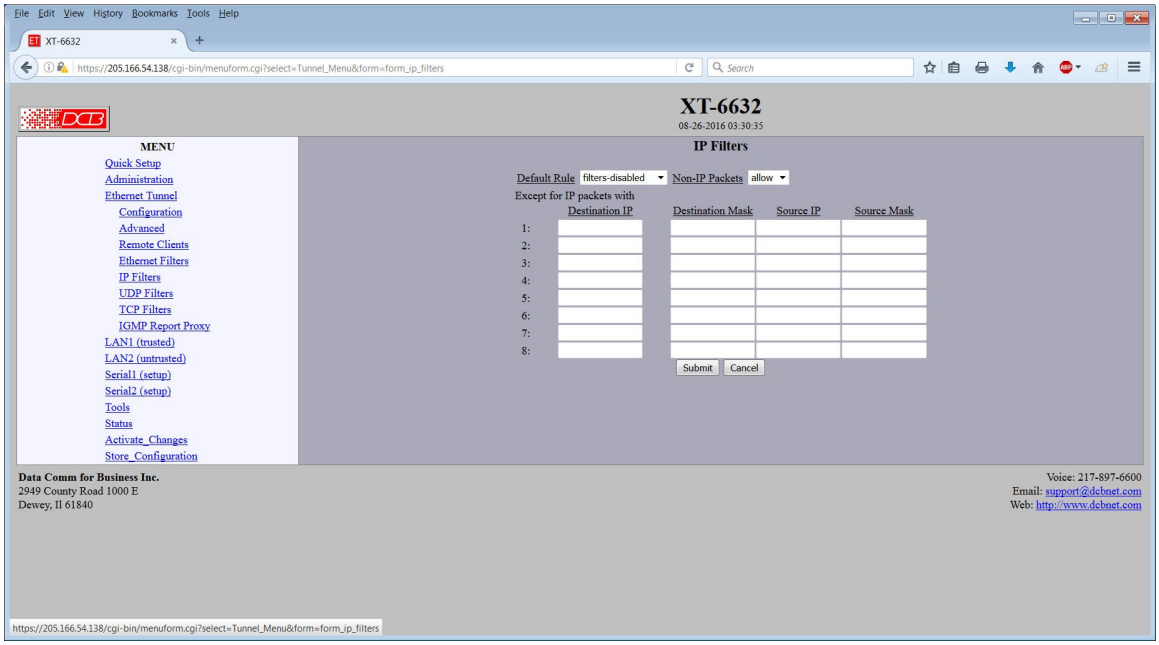
Fields

- Default Rule
  The table may be configured with the defaults of "allow all packets except", "drop all packets except", or filters disabled.
- Destination Address
  This field specifies the destination Ethernet address. If blank, it is interpreted to mean *any* address. The Ethernet address is a 6 byte number entered as 12 hexadecimal digits, with each byte optionally separated with a ':', '-', or ' ' character. For example, 00:06:3B:00:17:01, 00-06-3b-00-17-01, 00 06 3b 00 17 01, 00063b001701 are all valid input.

- Source Address
  This field specifies the source Ethernet address. If blank, it is interpreted to mean *any* address. See above for formatting examples.
- Protocol
  This field specifies the Ethernet Protocol ID. It is entered as a 4 digit hexadecimal number. The valid range is 0600 to FFFF. Example values are 0800 - IP, 0806 - ARP, 0835 - RARP, 8137 - IPX.

Notes

IP Address Filters Screen



IP Address Filters Screen

IP filters are used to limit the Ethernet packets sent from the local tunnel to a remote tunnel. This level of filtering is performed on IP(0800) and ARP(0806) packets by comparing the destination and source addresses against a table of rules.

To use IP filtering, you first select a default rule. That is, you choose to **allow all** IP packets by default, or to **drop all** IP packets by default.

Next, you enter one or more exceptions to the default rule. An exception consists of a destination and a source IP address. Any packet matching both the destination address and the source address will be considered an exception, causing the opposite of the default rule to be performed. Addresses are entered in *address, mask* format. This allows you to specify a single host address or a subnet range. An entry of 0.0.0.0, 0.0.0.0 will match any address

Please note that IP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

IP filtering is performed after Ethernet Filtering. Any packets discarded by Ethernet filtering will not reach IP filtering.

Fields

- Default Rule
  This field specifies the action to be taken when an IP or ARP packet does not meet any of the exception rules.
- Non-IP Packets
  This field specifies the action to be taken when an Ethernet packet is not an IP or ARP type packet. This is simply a shortcut to setting up Ethernet Filters to block all non 0800 and 0806 type packets.

- Destination IP Address
  This field specifies the Destination IP address for comparison with the packet. The Destination Mask is applied, allowing a single host or a subnet range. If blank, the field is assumed to mean any address and is the same as entering an IP of 0.0.0.0 and a mask of 0.0.0.0. If both the destination and source address is blank, the entire rule is ignored.
- Destination Address Mask
  This field specifies the address mask. The mask is logically ANDed with the Destination IP address to extract the significant portion of the IP address. If the mask is blank, but the IP address is not blank, the mask is assumed to be 255.255.255.255. In other words, the IP address is treated as a host address.
- Source IP Address
  This field specifies the Source IP address for comparison with the packet. The Source Mask is applied, allowing a single host or a subnet range. If blank, the field is assumed to mean any address and is the same as entering an IP of 0.0.0.0 and a mask of 0.0.0.0. If both the destination and source address is blank, the entire rule is ignored.
- Source Address Mask
  This field specifies the address mask. The mask is logically ANDed with the Source IP address to extract the significant portion of the address. If the mask is blank, but the IP address is not blank, the mask is assumed to be 255.255.255.255. In other words, the IP address is treated as a host address.

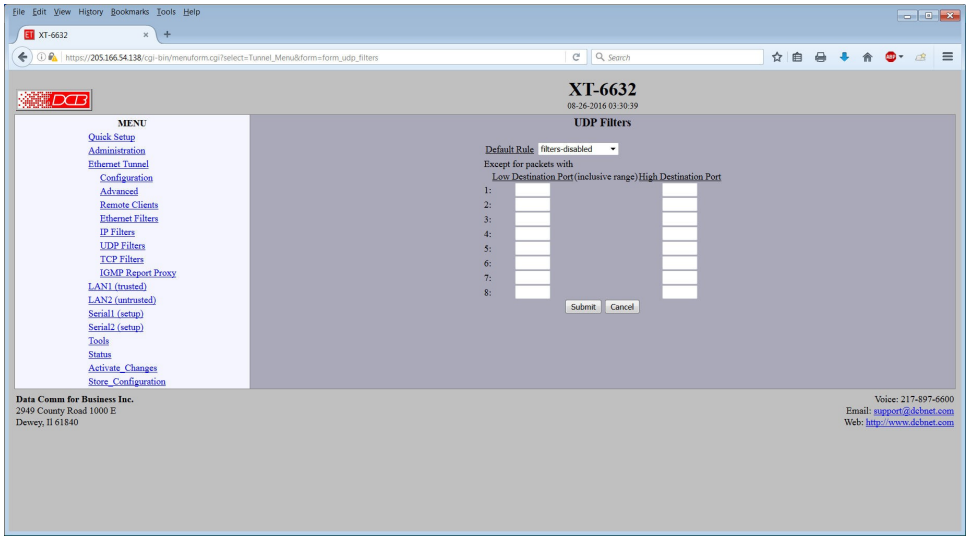
Notes

Please note that IP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

IP filtering is performed after Ethernet Filtering. Any packets discarded by Ethernet filtering will not reach IP filtering.

Please note that IP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

UDP Filters Screen



UDP Address Filters Screen

UDP filters are used to limit the UDP packets sent from the local tunnel to a remote tunnel. This level of filtering is performed on the UDP Destination Port Number. It would typically be used to eliminate certain types of UDP broadcasts. For example, you may not want DHCP requests to cross between local and remote networks. In this case you would block UDP ports 67 and 68.

To use UDP filtering, you first select a default rule. That is, you choose to **allow all** UDP packets by default, or to **drop all** UDP packets by default.

Next, you enter one or more exceptions to the default rule. An exception consists of a range of destination port numbers. Any UDP packet with a destination port number in the specified range will be considered an exception, causing the opposite of the default rule to be performed.

Please note that UDP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

UDP filtering is performed after IP Filtering. Any packets discarded by IP filtering will not reach UDP filtering.

Fields

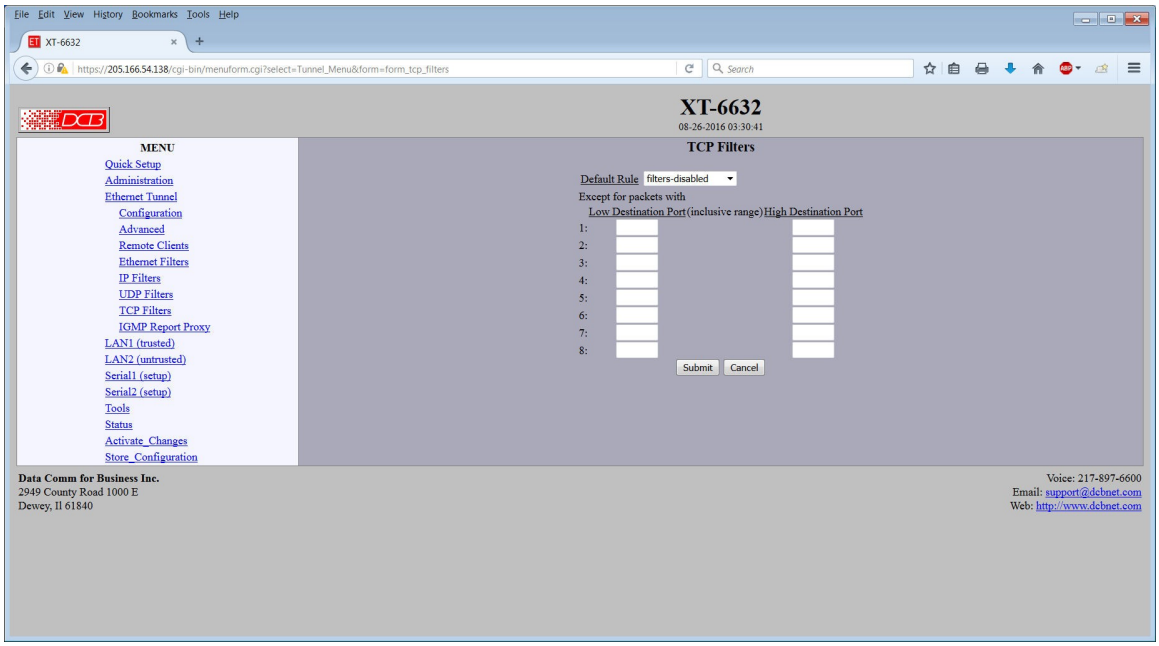
- Default Rule
  This field specifies the action to be taken when an UDP packet does not meet any of the exception rules.
- Low Destination Port
  This field specifies the Low Destination Port Number in an inclusive range. If you only wish to specify one port number, place that port number in both the low and high field.
- High Destination Port
  This field specifies the High Destination Port Number in an inclusive range. If you only wish to specify one port number, place that port number in both the low and high field.

Notes

Please note that UDP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

UDP filtering is performed after IP Filtering. Any packets discarded by IP filtering will not reach UDP filtering.

TCP Filters Screen



TCP Address Filters Screen

TCP filters are used to limit the TCP packets sent from the local tunnel to a remote tunnel. This level of filtering is performed on the TCP Destination Port Number. It would typically be used to eliminate a specific service. For example, you may not want Telnet requests to come in from a remote network. In this case you would block TCP port 23 in the remote tunnel device.

To use TCP filtering, you first select a default rule. That is, you choose to **allow all** TCP packets by default, or to **drop all** TCP packets by default.

Next, you enter one or more exceptions to the default rule. An exception consists of a range of destination port numbers. Any TCP packet with a destination port number in the specified range will be considered an exception, causing the opposite of the default rule to be performed.

Please note that TCP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

TCP filtering is performed after IP Filtering. Any packets discarded by IP filtering will not reach TCP filtering.

Fields

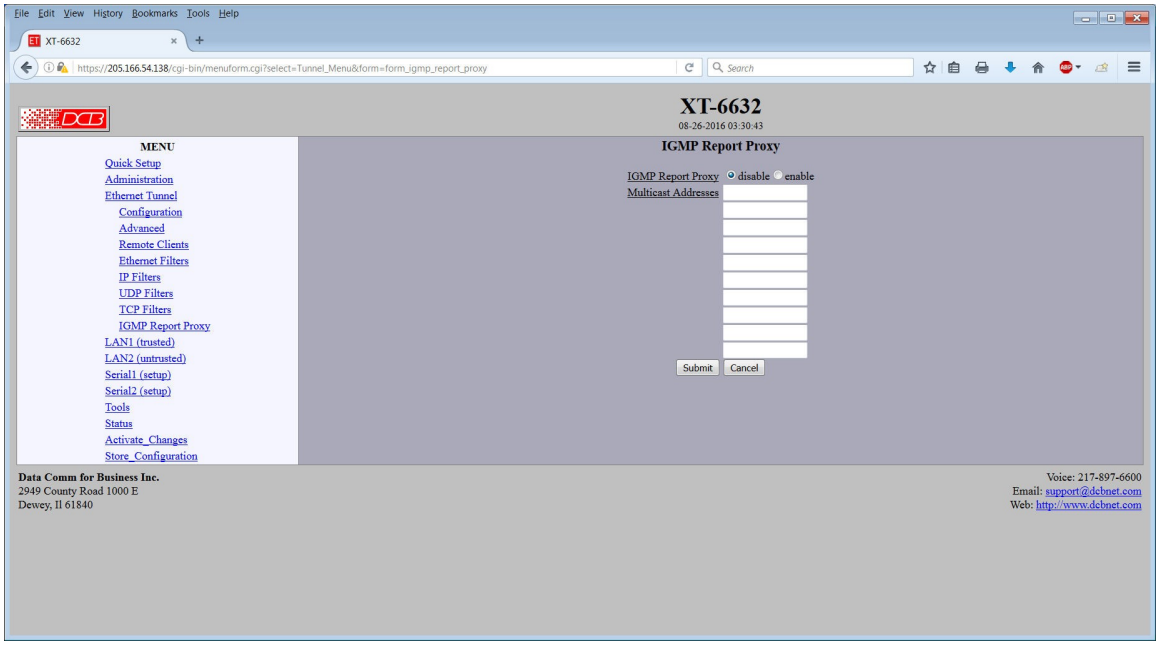
- Default Rule
  This field specifies the action to be taken when an TCP packet does not meet any of the exception rules.
- Low Destination Port
  This field specifies the Low Destination Port Number in an inclusive range. If you only wish to specify one port number, place that port number in both the low and high field.
- High Destination Port
  This field specifies the High Destination Port Number in an inclusive range. If you only wish to specify one port number, place that port number in both the low and high field.

Notes

Please note that TCP filtering is only applied to packets traveling in from the local Ethernet toward a remote tunnel.

TCP filtering is performed after IP Filtering. Any packets discarded by IP filtering will not reach UDP filtering.

IGMP Report Proxy



IGMP Report Proxy Configuration Screen

IGMP snooping and protocols such as PIM rely on IGMP reports to build their forwarding tables. However some multicast receivers do not fully implement IGMP, resulting in the multicast packets not reaching the physical network segment. To work around this problem the tunnel can be configured to "join" a set of multicast channels. It will then generate the proper IGMP reports.

IGMP Report Proxy should be enabled in the tunnel on the same physical LAN as the multicast receiver.

IGMP Report Proxy will not correct a situation where an IGMP snooping Ethernet switch is placed between the tunnel and the multicast receiver. IGMP snooping will need to be disabled in the Ethernet switch.

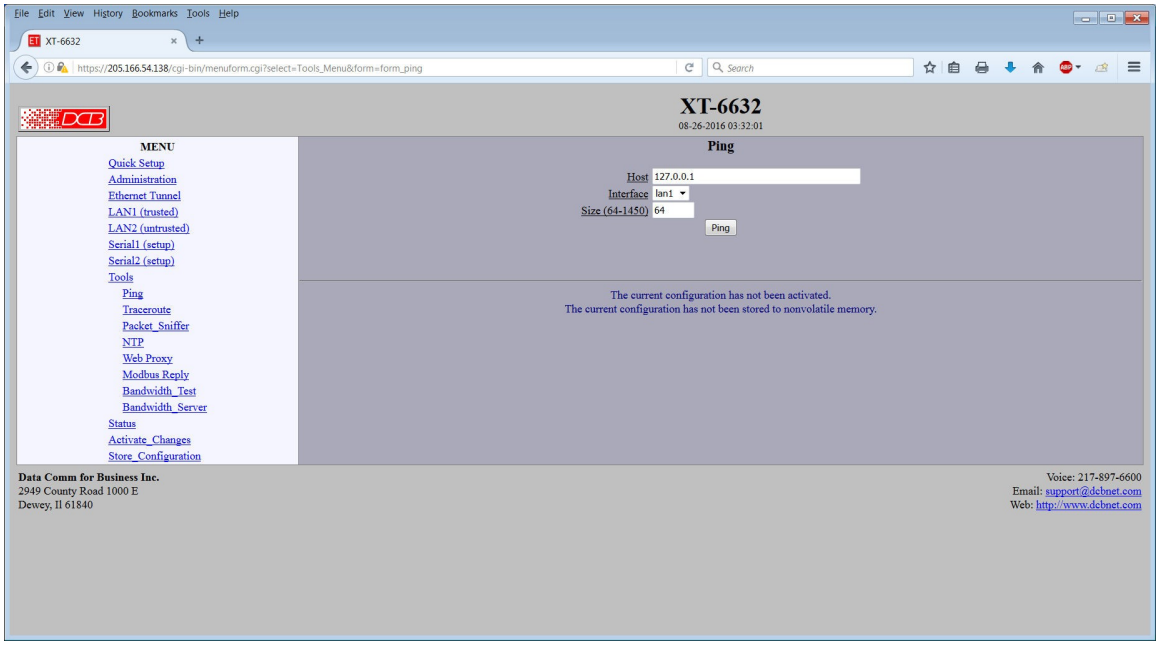
Fields

IGMP Report Proxy
This Enables or disables IGMP Report Proxy

Multicast Addresses
This is list of multicast addresses to join.

Notes

Ping Screen



Ping Screen

Ping will send four ICMP echo requests to the specified host. It will wait approximately 16 seconds for a response.

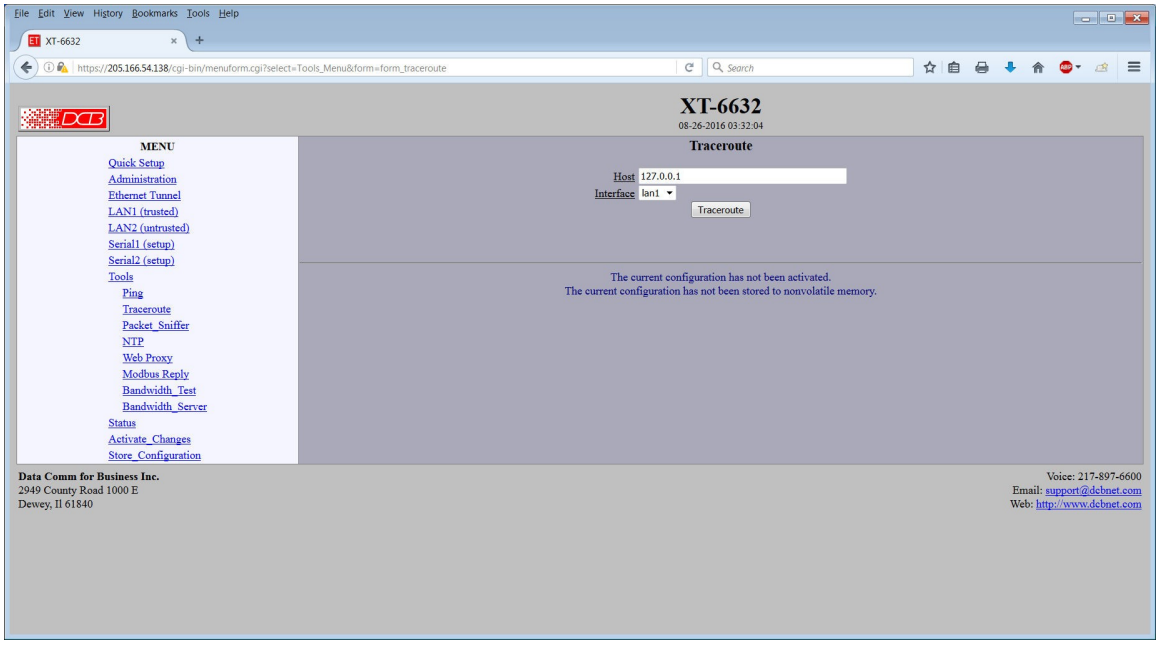
Fields

- Host
  IP address of the target host. If hostname DNS is enabled, you may use a host name.
- Interface
  Which interface to use. This controls the default gateway to be chosen in the event the target host is not on a local network segment.
- Size
  Number of data bytes to send.

Notes

- Ping and traceroute are useful tools to determine if routing is correct.

Traceroute Screen



Traceroute Screen

Traceroute displays the route that a packet will take to reach another host. This is performed by sending UDP packets to port 33434 with progressively larger Time-to-Live values and listening for ICMP TIME-EXCEEDED responses from the bridges along the way.

Fields

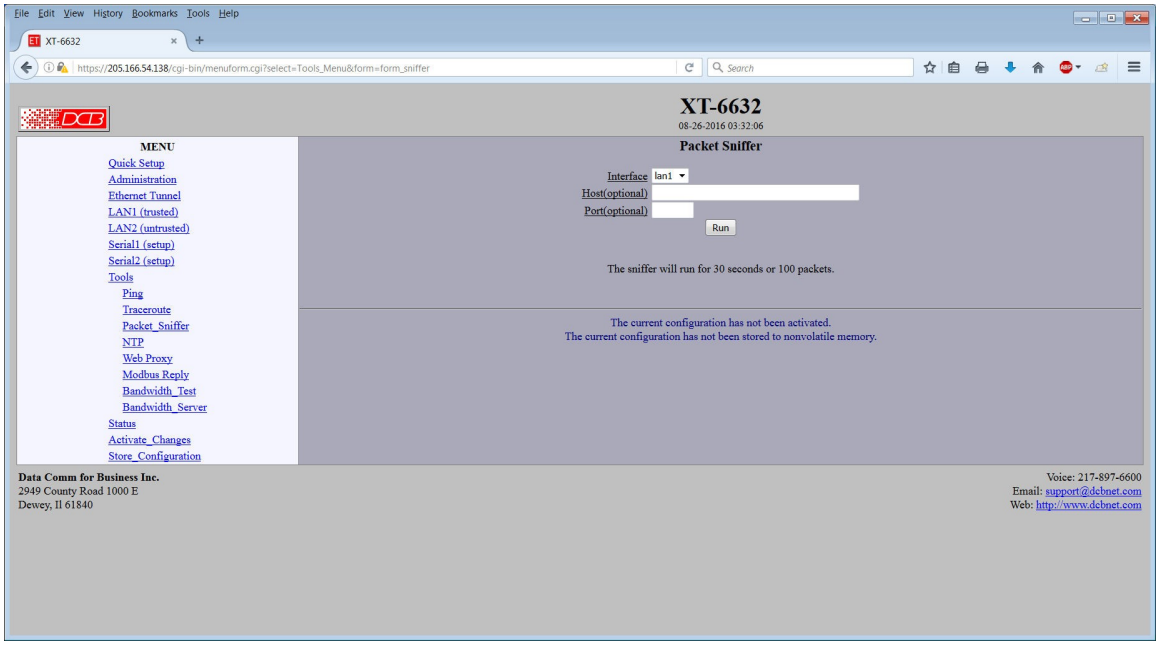
Host

IP address of the target host. If hostname DNS is enabled, you may use a hostname.

Interface
Which interface to use. The routing table is bypassed.

Notes

Packet Sniffer Screen



Packet Sniffer Screen

The Packet Sniffer allows you to take a snapshot of the network traffic passing through an interface.

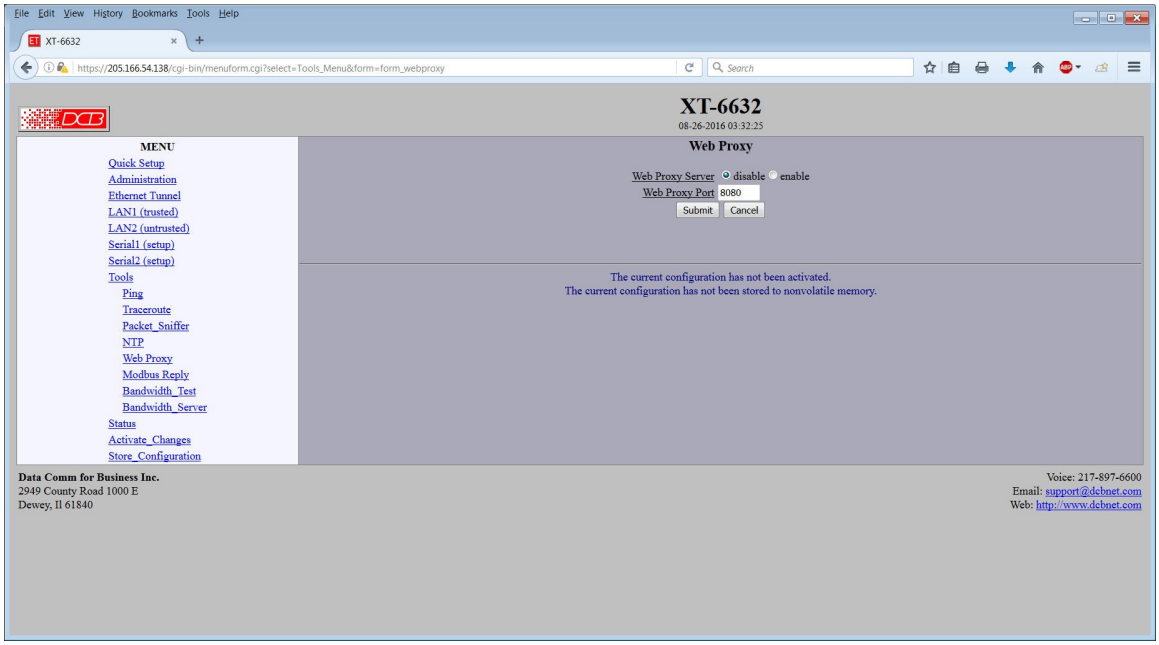
Fields

- Interface
  Which interface to use. If the interface is a serial port, you will only see the traffic that is passing through the IP layer of PPP. You will not see low-level PPP traffic.
- Host
  This applies a host filter. Only packets with a matching source or destination IP address will be included in the trace.
- Port
  This applies a port number filter. Only TCP or UDP packets with a matching source or destination port number will be included in the trace..

Notes

- Only packet headers are shown. You will not be able to see the data contents of the packets.

Web Proxy Configuration Screen



Web Proxy Configuration Screen

The Web Proxy Server allows you to use the tunnel as a light weight local HTTP proxy, directing HTTP requests directly onto the insecure network instead of tunneling them to your remote network. It is not designed to be useds as a high performance general purpose web proxy.

The Web Proxy server can be helpful when using the tunnel on a captive untrusted network, which requires authentication before access is allowed to the Internet or for configuring network equipment on the untrusted network.

In order to use the web proxy server, you will need to configure your web browser. For Internet Explorer, this can be found in Tools - Internet Options - Connections - LAN Settings. For Firefox, this can be found in Edit - Preferences - Connection Settings. Do not use the auto-detect feature. Manually set the IP address and port number. Use the IP address of the Ethernet-A interface as the proxy server address.

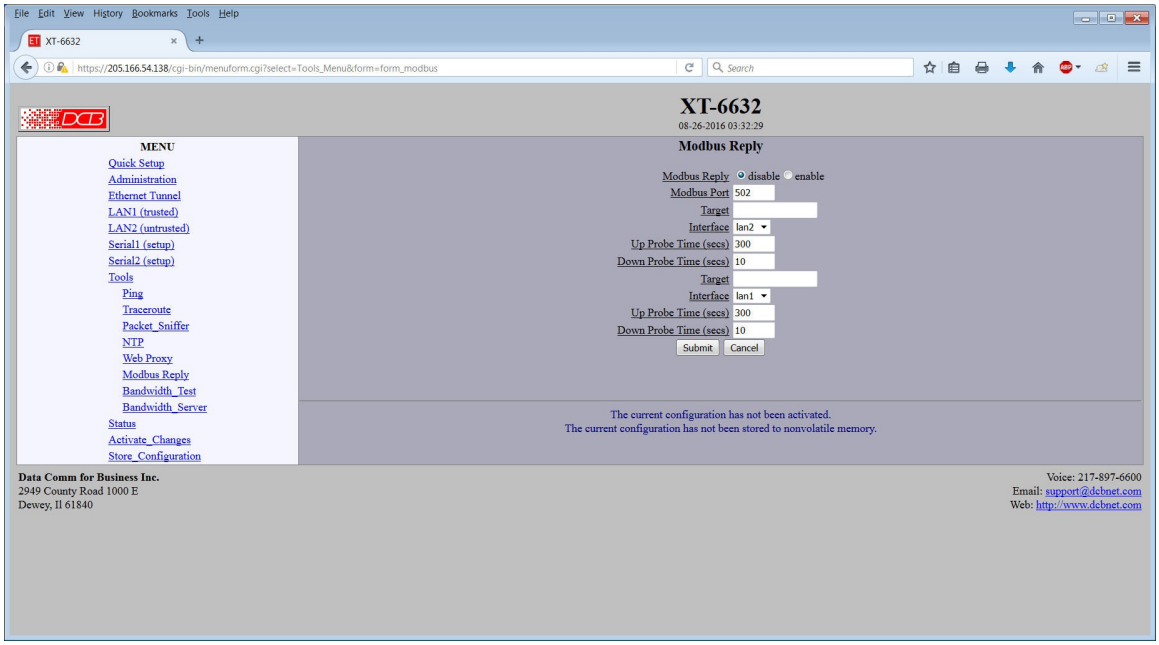
Fields

- Web Proxy Server
  This item enables/disables the web proxy server.
- Web Proxy Port
  The TCP port number that the web proxy will listen to for connection requests. This will need to match the port number in your web browser's configuration.

Notes:

- In order to use the web proxy server, you will need to configure your web browser. For Internet Explorer, this can be found in Tools - Internet Options - Connections - LAN Settings. For Firefox, this can be found in Edit - Preferences - Connection Settings. Do not use the auto-detect feature. Manually set the IP address and port number. Use the IP address of the Ethernet-A interface as the proxy server address.

Modbus Reply Configuration Screen



Modbus Reply Configuration Screen

The Modbus Reply feature allows the XT device to be monitored using the Modbus/TCP protocol. The XT device will report the status of 4 items using the following modbus registers:

```
10001   Tunnel Mode    0=Server,          1=Client
10002   Target-1       0=Not Responding,  1=Responding
10003   Target-2       0=Not Responding,  1=Responding
10004   Tunnel Client  0=On Backup,       1=On Primary.
```

The above information is also reported on modbus registers 20001 - 20004, 30001 - 30004, and 40001 - 40004.

Note: If the XT device is configured for both Server and Client mode, register 10001 will report 1. If the XT device is configured for Server mode, register 10004 will always report as 1.

Fields

Modbus Reply
Enables or disables the Modbus Reply feature.

Modbus Port

This field selects the TCP port to use for Mobus Requests. Port 502 is the standard port number for Modbus/TCP

Target IP
This field sets the IP address of a target device. A ping (ICMP echo) packet will be sent to this target at a periodic rate. If the target responds to the ping, the target will be reported as responding. If the target fails to respond to 3 sequential ping requests, the target will be reported as not responding.

Interface LAN UP Probe Time (secs)

This field sets the rate that ping packets will be sent to the target when the target is responding.

D**own Probe Time (secs)**

This field sets the rate that ping packets will be sent to the target when the target is not responding. It is also used as the timeout for determining a missed response. If the target fails to respond to a ping packet for 3 times the *down_probe* time, the target will be flagged as not responding in the modbus reply.

Target IP
This field sets the IP address of a target device. A ping (ICMP echo) packet will be sent to this target at a periodic rate. If the target responds to the ping, the target will be reported as responding. If the target fails to respond to 3 sequential ping requests, the target will be reported as not responding.

Interface LAN UP Probe Time (secs)

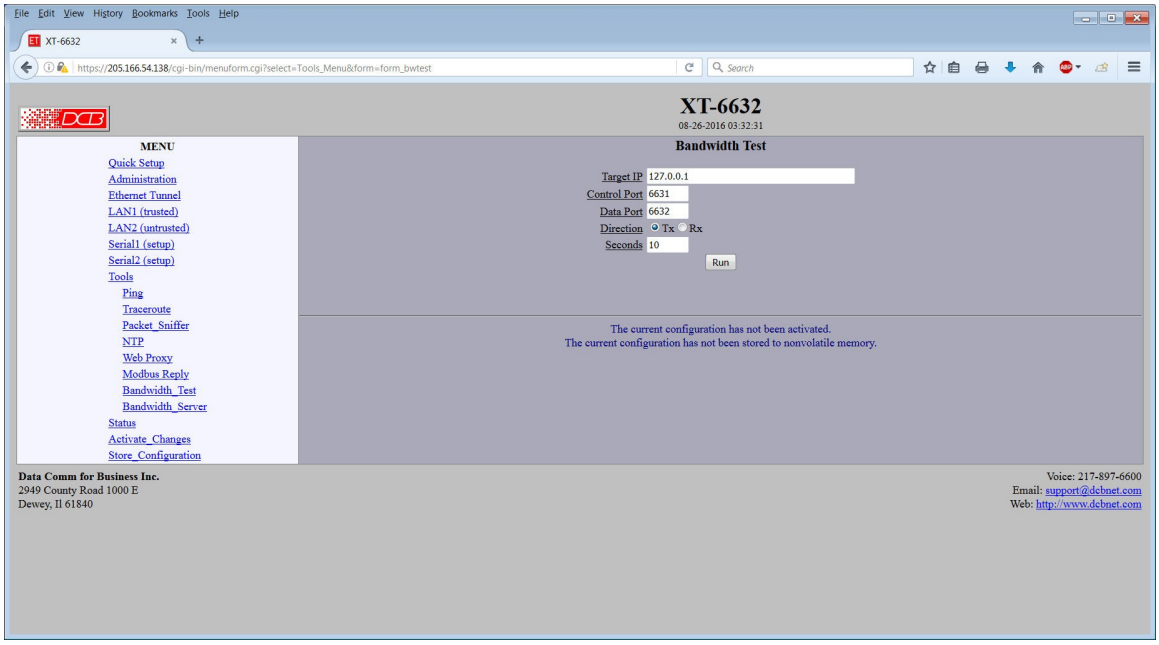
This field sets the rate that ping packets will be sent to the target when the target is responding.

D**own Probe Time (secs)**

This field sets the rate that ping packets will be sent to the target when the target is not responding. It is also used as the timeout for determining a missed response. If the target fails to respond to a ping packet for 3 times the *down_probe* time, the target will be flagged as not responding in the modbus reply.

Notes:

Bandwidth Test



Bandwidth Test Screen

This tool runs the client side of the NutTCP network test utility. It is run in TCP mode to measure the bandwidth between the client and the server devices.

Fields

Target IP
IP address or host name of the target device to run the bandwidth test against. The target device must have the NutTCP server running.

Control Port

The control port number to use for connecting to the NutTCP server. The target device NutTCP server must be configured with the same control port number.

Data Port
The data port number to use for connecting to the NutTCP server.

Direction

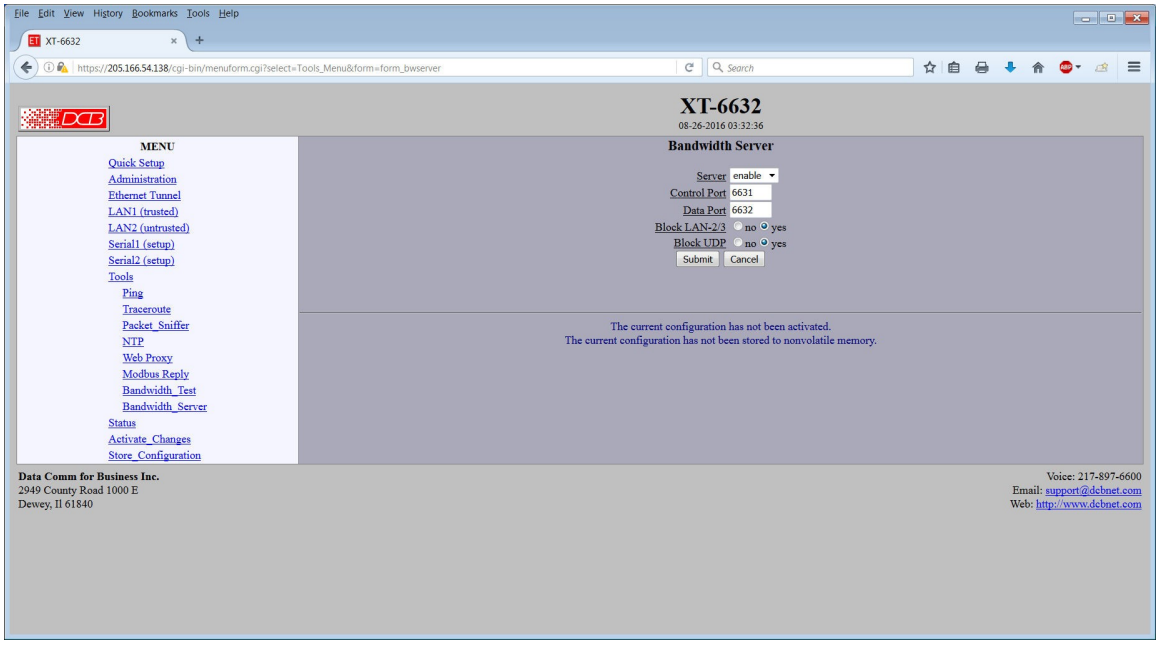
This field selects the direction of the data transfer test with respect to the NutTCP client.

Seconds

This field sets the duration of the data transfer in seconds. Duration may be set from 1 to 20 seconds.

Notes:

Bandwidth Server



Bandwidth Server Screen

This tool enables the server side of the NutTCP network test utility.

Fields

Server
Enable/disable the NutTCP server. When the NutTCP server is enabled but not in use, it uses little system resources. So it is OK to always have it enabled. However, if you do enable it, it is recommended to firewall it from LAN-2 access by enabling the Block LAN-2 option.

Control Port

The control port number to listen to for client connections. The NutTCP client must use this same port number.

Data Port
The data port number to expect the NutTCP client to use. This port number does not directly apply to the NutTCP server. However, to properly firewall LAN-1, this should be set to the same port number used by the NutTCP client.

Block LAN2

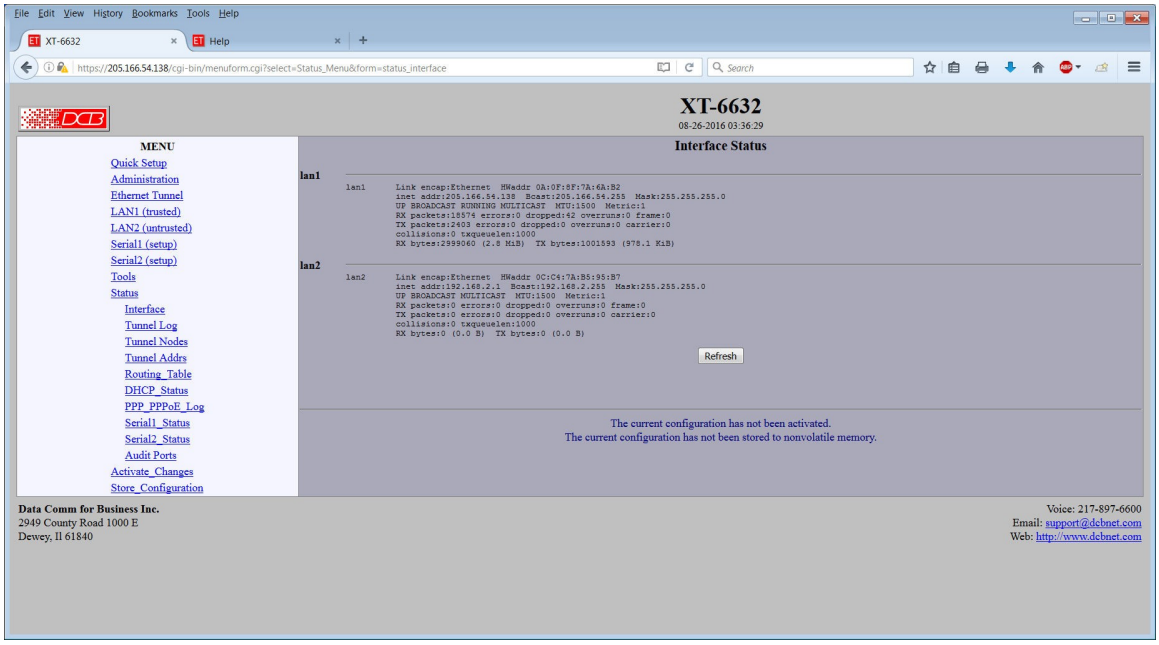
When set to *yes*, firewall rules will be applied blocking access to the NutTCP server via LAN-2.

Block UDP

NutTCP supports both TCP and UDP testing. When set to *yes*, firewall rules will be applied blocking UDP access to the NutTCP server.

Notes:

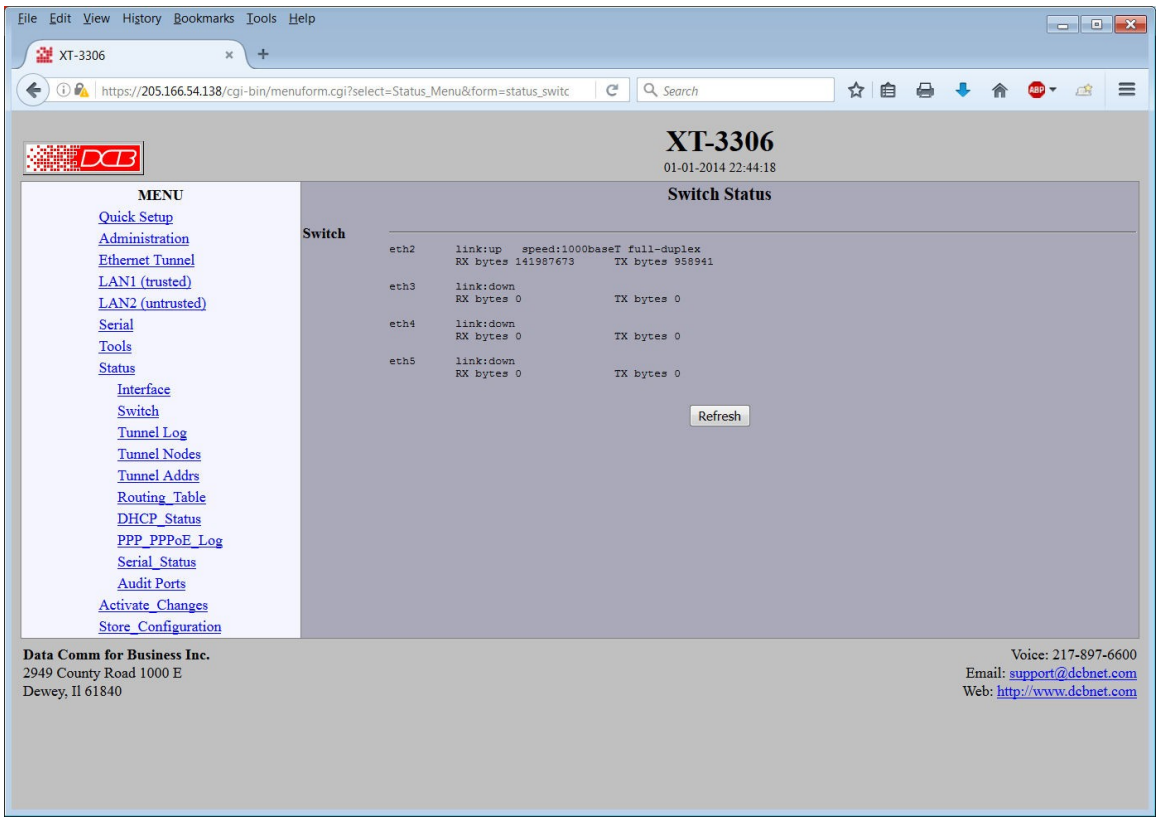
Interface Status Screen



Interface Status Screen

The Interface Status screen shows port status and packet counters for each interface on the XT. The page is static and the Refresh button must be clicked to update the counters.

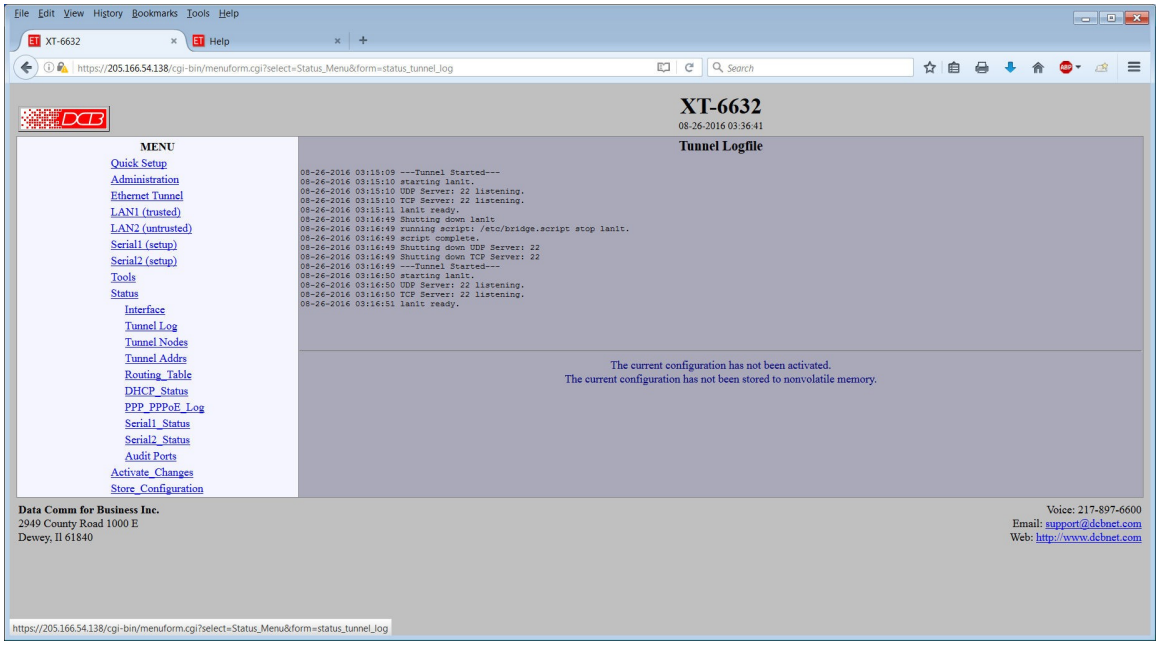
Switch Status Screen



Switch Status Screen

Available on units containing an integral switch, the Switch Status screen shows link information for each ethernet switch port including link status, receive and transmit bytes. This is a static screen and must be refreshed to update.

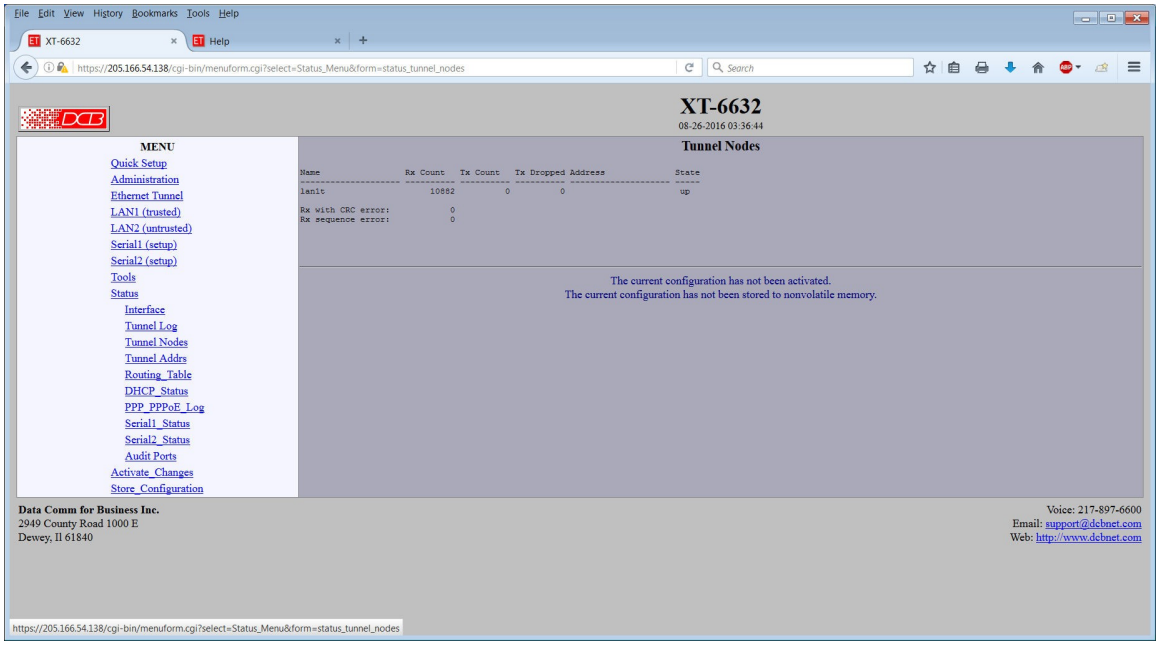
Tunnel Log Screen



Tunnel Log Screen

The Tunnel Log screen shows important events logged for each interface on the XT.

Tunnel Nodes Screen



Tunnel Nodes Screen

The Tunnel Nodes screen shows the status of known remote XT nodes. Status is indicated by the state being UP, connecting, or connected. This screen also displays two error counters. Errors in either of these counters indicate a problem on the network between this bridge and it's peer, not a problem within the bridges.

Fields

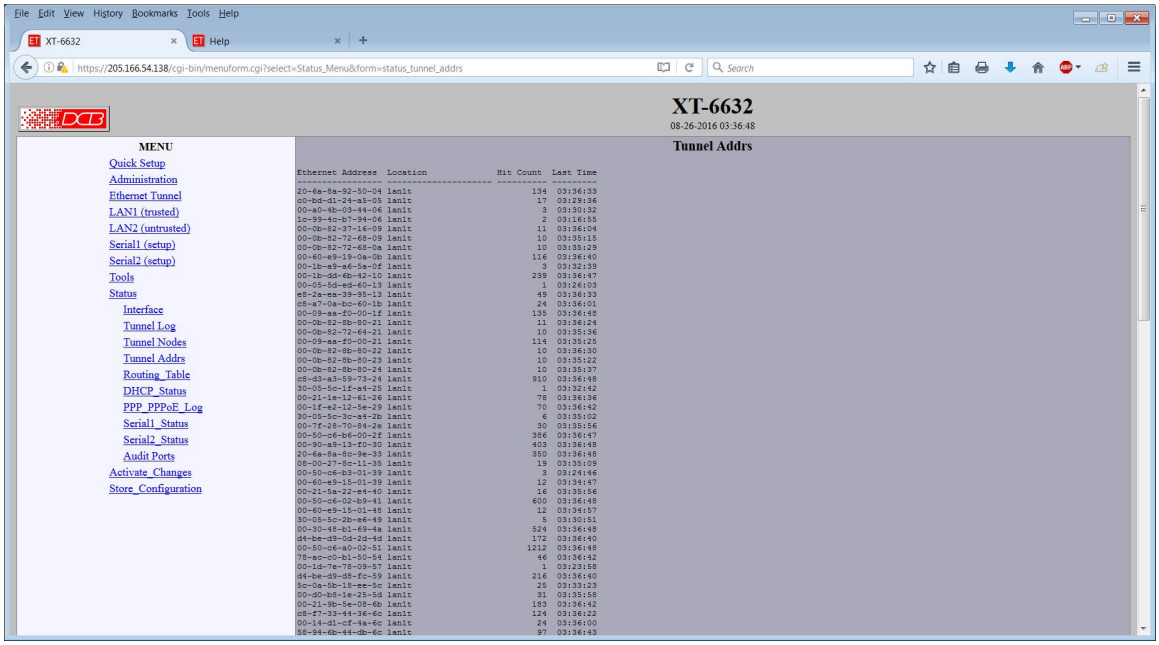
Rx with CRC error:

CRC Errors indicate a failed CRC calculation on the payload of the incoming packet. This could be due to in-transient packet fragmenting and not all the packets being delivered, in which case the original packet can't be reconstructed.. creating the CRC error. This can sometimes be mitigated by enabling the “Limit UDP Packet Size” in the Ethernet Advanced Configuration screen. Less likely causes might be spoofing; or port scanning.

Rx sequence error:

Sequence Errors indicate out-of-order packets being received since each packet is numbered sequentially. This may be from intermediate routers or bridges duplicating packets, which is most common on wireless links, or dropped packets, sometimes caused by network conjestion. Rarely, it may also be caused by a MIM attack with packet spoofing. It's almost always a problem caused by having a wireless link in the middle.

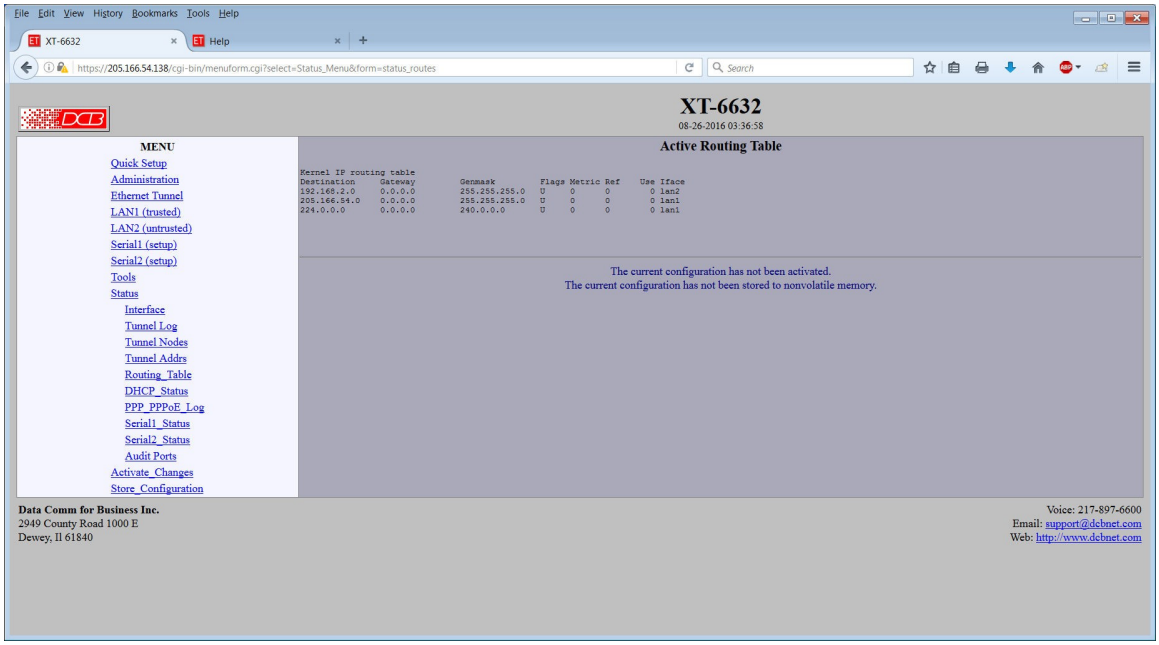
Tunnel Addresses Screen



Tunnel Addresses Screen

The Tunnel Addresses screen shows the ethernet (MAC) address of all ethernet nodes recognized along with their port location, hit count, and time of last contact.

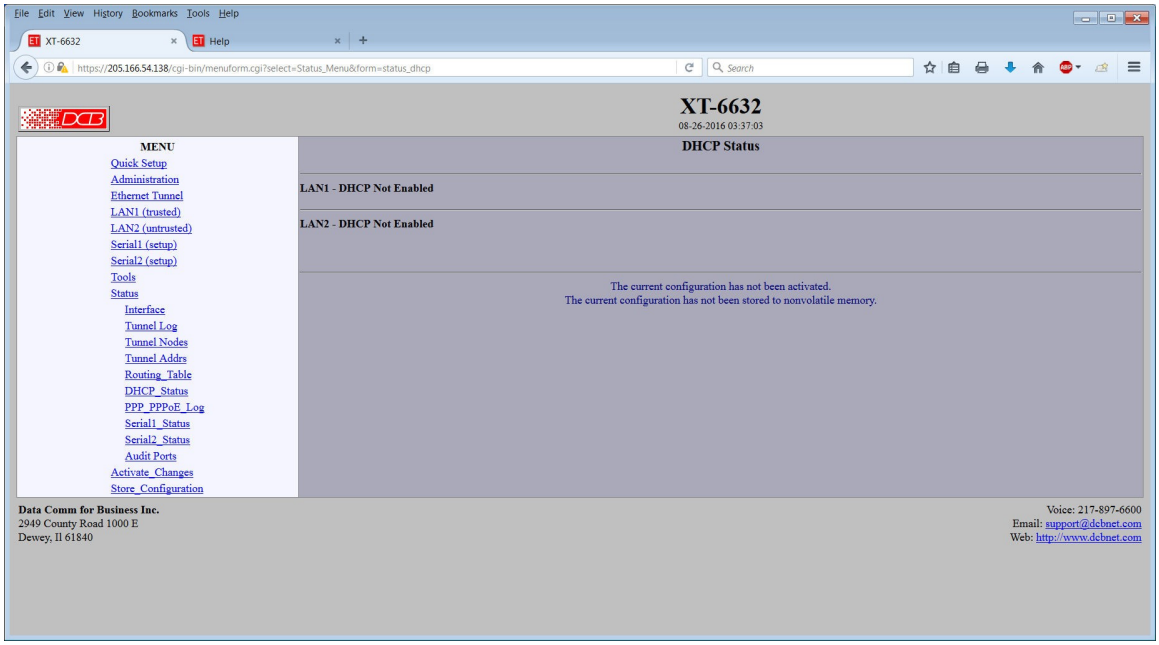
Routing Table Screen



Routing Table Screen

The Routing Table screen shows all routes configured in the XT.

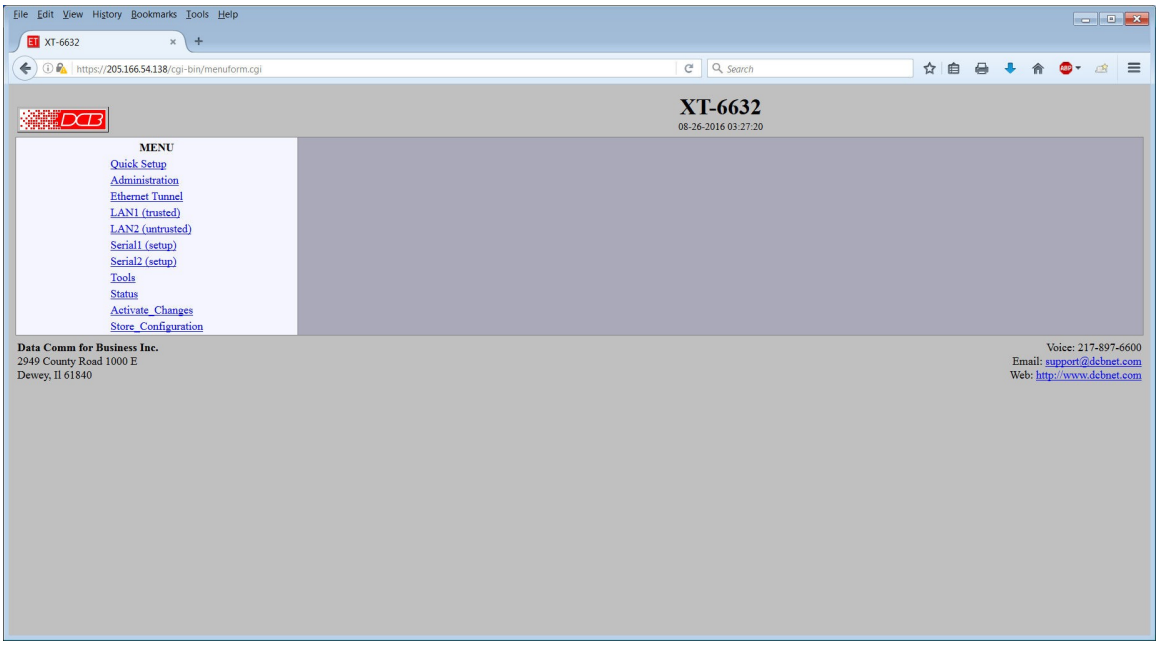
DHCP Status Screen



DHCP Status Screen

The DHCP Status Screen displays recent history of DHCP server activity.

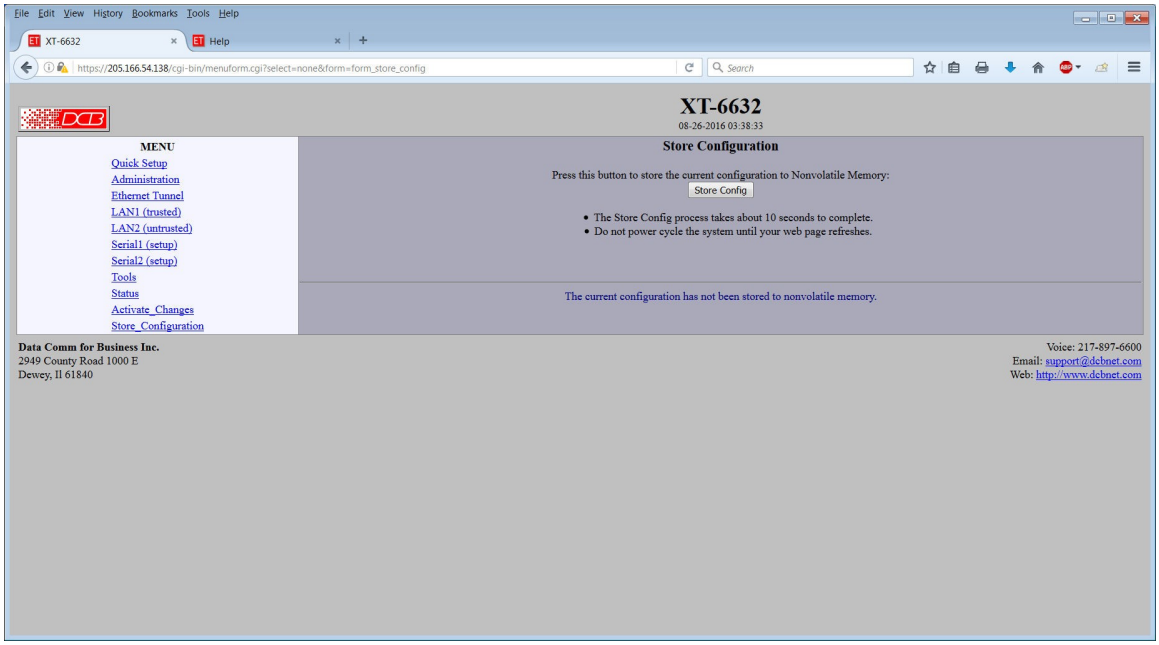
PPPOE Log Screen



PPPoE Log Screen

The PPP Log Screen displays recent history of PPPoE operation if PPPoE is enabled.

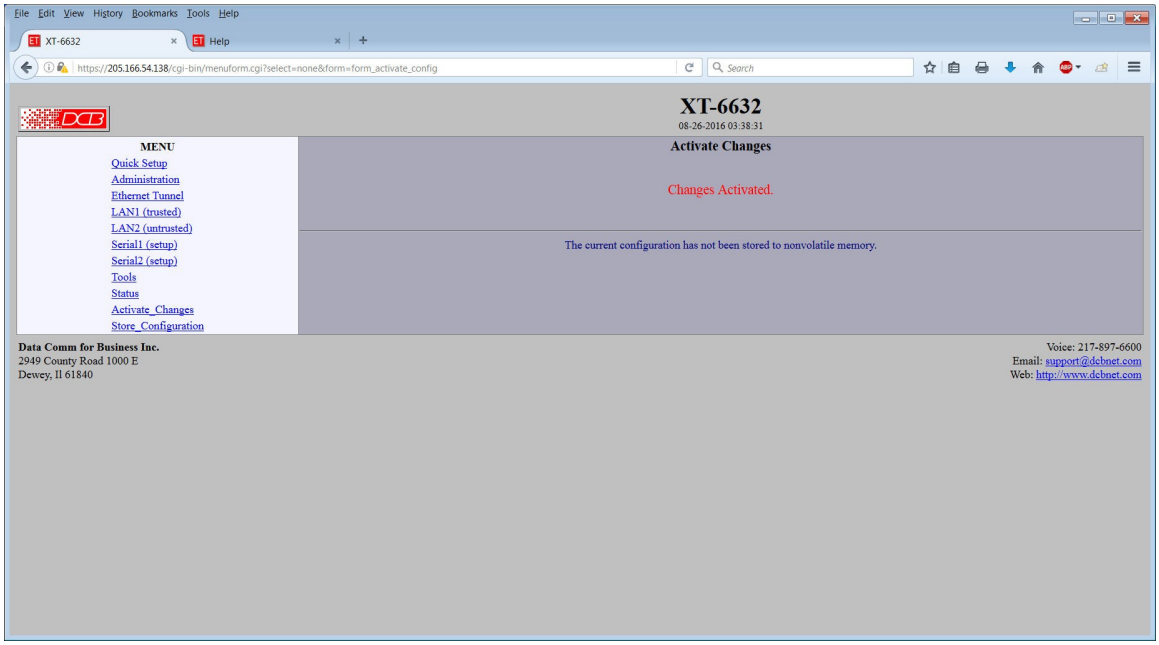
Store Configuration Screen



Store Configuration Screen

The Store configuration screen is used to store the current configuration to non-volatile memory. This does not activate configuration changes. Configuration changes are made to a temporary area. They may be "activated" using the Activate Changes screen, in which case they will become immediately active, overwriting the pre-existing configuration for the duration of this session; or they may be "stored" using this screen, in which case they will be written to non-volatile memory and used at the next reset or power-up. **Refer to the configuration process section for details about the configuration process.**

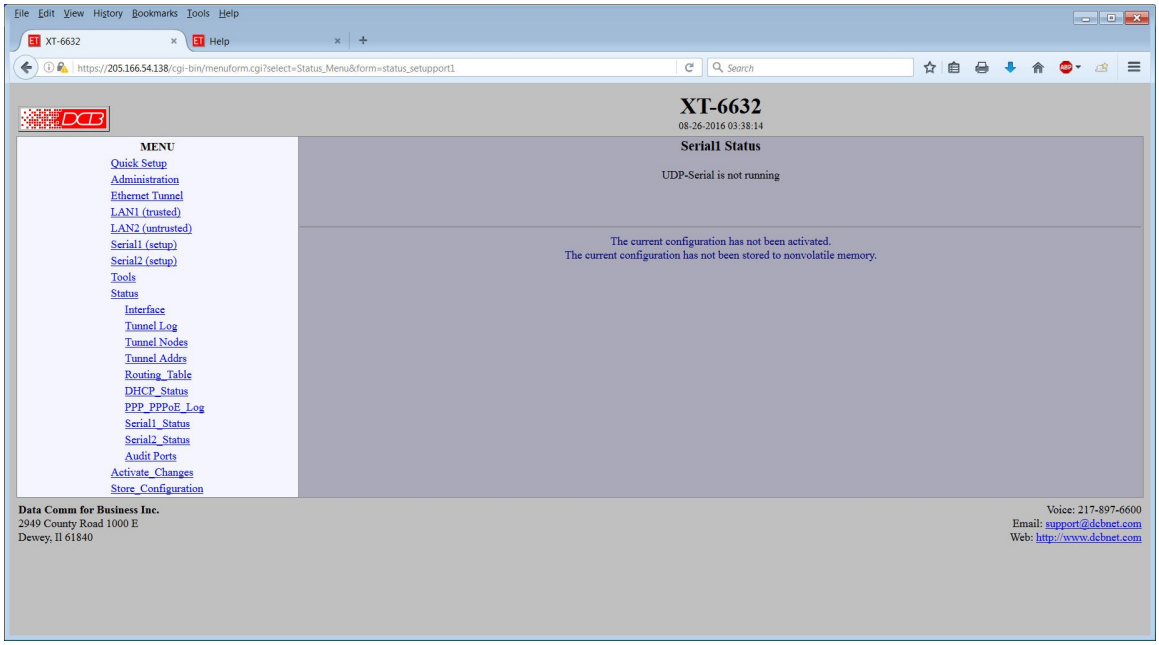
Activate Configuration Screen



Activate Configuration Screen

The Activate Changes screen is used to activate the current changes. Configuration changes are made to a temporary area. These changes will become immediately active, overwriting the pre-existing configuration for the duration of this session. Changes may be "stored" using the store configuration screen, in which case they will be written to non-volatile memory and used at the next reset or power-up.

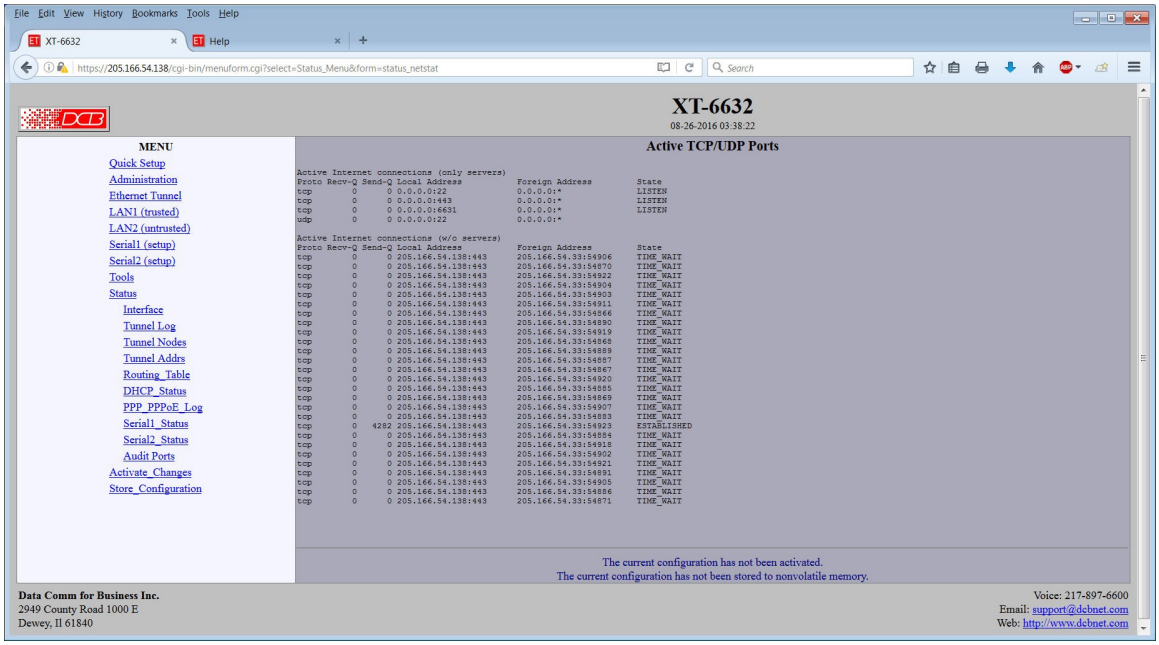
Serial Status



Serial Status Screen

This screen displays the status of the UDP or TCP serial server for the serial ports.

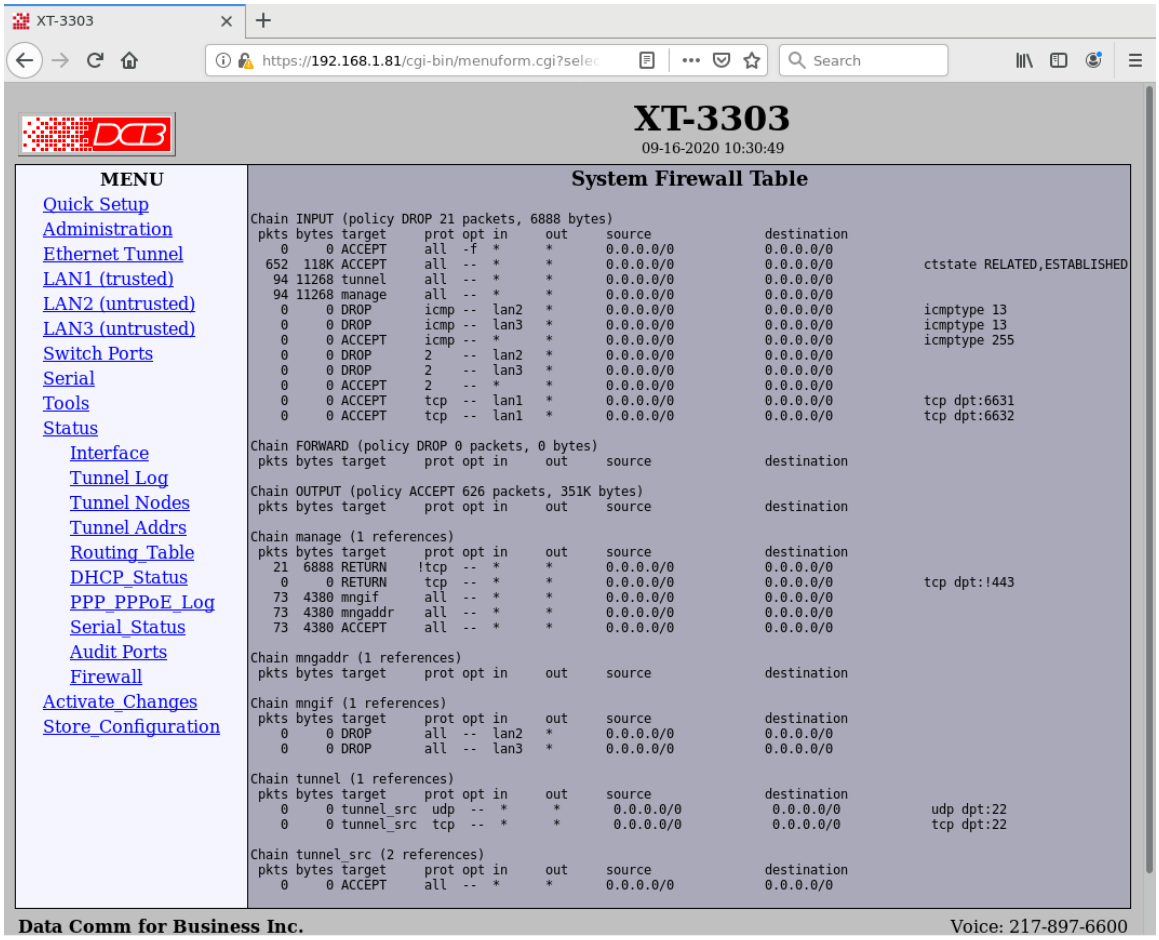
Audit Ports Screen



Audit Ports Screen

The Audit Ports screen displays a list of all active TCP and UDP connections along with their state.

Firewall Status



Firewall Status Screen

The Firewall Status screen displays the unit's active Linux Firewall. The firewall configuration is automatically built based on the unit configuration. These are the policies and rules intended to protect the underlying Linux system. This status display is intended as an aid to users performing security audits on the device. An understanding of Linux IPTables and NetFilters is required to interpret the table.

Chapter 5
Operation

This Chapter explains how to use the XT, once it is installed and configured.

Common Uses – Overview

Some of the most commonly used configurations are for:

- Remote LAN connected to local LAN via broadband, satellite, cable, wireless, or wired ISP Internet connection
- Remote LAN connected to local LAN via a captive enterprise WAN connection
- Multiple remote LANs connected together using various ad-hoc ethernet connections

Any of these connection methods may have the data transverse the Internet, a private network, various firewalls, NAT servers, and other routes. Although any ethernet protocol may be bridged (including UDP, IP, Netbios, Appletalk, etc) the connection between two XT units is via UDP/IP, therefore a TCP path is required between the XT units.

These configurations are detailed in this chapter. Some sample configuration files may be downloaded from the DCB support web site and then transferred to your bridge.

The local or remote LAN may be a full-fledged network or a single ethernet device using an ethernet cross-over cable.

The XT link requires one unit to be configured as a server, and one or more units configured as clients. A single XT may function as both a server and a client.

Remote LAN to Local LAN via Broadband Internet

The server XT is connected to the main site LAN and eventually connected to the Internet via some ISP. The remote client XT is connected to a broadband router via LAN2, and a local LAN is connected to LAN1. All ethernet devices on the local LAN are bridged to the remote LAN. Filtering may be used to limit connectivity to the desired ethernet devices. When the units power up, the remote XT automatically connects to the server XT with a persistent connection.

Remote LAN to Local LAN via Wireless Internet

Similar to the above configuration, but a wireless ethernet device is used in the public Internet connection path. The remote LAN may use either a hardware XT or the UT-Soft software client. This method is often used for temporary and mobile applications using AIR cards or cellular broadband.

Remote LAN to Local LAN via Ad-hoc connections

As in the above configurations, except there are multiple XT remote locations that are used “ad-hoc”, and with DHCP providing local IP configuration and the path back to the host XT. By configuring LAN2 on

the remote XT bridges to use DHCP, the remote LAN is highly portable and can be installed and used without reconfiguring for each remote location.

Typical Application Diagrams

Some application diagrams may be displayed by pressing the “Press here for application diagrams” link on the Quick Setup Screen.

Application Notes

There are numerous application examples and app notes available on the Data Comm for Business Web site. These may be downloaded from the product data sheets at http://www.dcbnet.com

Chapter 6
Troubleshooting

This chapter outlines some problems that may occur during installation or operation and some possible solutions to them.

If you follow the suggested troubleshooting steps and the XT bridge still does not function properly, please contact your dealer for further advice.

Hardware Problems

Before anything else, check that all cables are wired correctly and properly connected.

***P*:** All the LEDs are off.
S: Check the power supply or power connection.

***P*:** When using 10/100/1000Base-T cabling, the unit does not work.
S: Check the switch's link LED for the port to which the bridge is connected. If it is off, make sure the network cable between the bridge and hub is in good condition.

Can't Connect via the LAN

***P*:** Can't connect with a Web Browser.
S: Check the following:

- Insure that you are addressing the XT correctly ie. https:// instead of http:// for some models .
- Start troubleshooting from a known state. Power everything OFF and ON to reboot.
- Is a proper IP address configured in the bridge and PC?
- "Ping" the bridge to see if it responds. From the Windows command prompt or "Run" dialog box, use the command:

  ```
  ping IP_Address
  ```

  Where `IP_Address` is the IP Address of the bridge (e.g. `ping 192.168.0.1`). If it does not respond, then check all LAN connections. If the LAN connection are OK, the problem is in the LAN addresses or routing **The most common problem cause is incorrect IP address configurations. Make sure the workstation and bridge have compatible IP addresses.**
- It may be that your workstation "ARP table" contains invalid entries. You can clear the "ARP table" by rebooting, or, on Windows, by typing the following command at the command prompt or *Run* dialog box.: `ARP * -d` **. This is a common problem with test-bench setups.**
- In some cases, switches must be power-cycled to clear their internal ARP cache. **This is often a problem on test bench setups where IP addresses are moved between different equipment or a unit is moved between ethernet switch receptacles.**

Other Problems

***P*:** Can't run the initial configuration program using a serial cable connection.

S: Check that:

- The communication parameters are set properly and a null cable is used.
- Power is available... an LED is on.
- The terminal program is operating properly. Try a loopback connector at the bridge end of the cable to verify program operation and the proper COM: port.
- The most common problems causing this symptom are incorrect RS-232 wiring or the Windows Hyperterm program not operating correctly.

***P*:** How to set the bridge back to factory defaults?
S: If you know the IP address, you may browse to the Administration screen – Set All Defaults. If the IP address is unknown and your unit contains a serial interface, use the serial connection setup method (Chapter 2), and answer Yes when asked if you wish to reset the unit to factory defaults. On an XT-3305, press the reset button for 5 seconds while powered on. The factory default IP address for the trusted side ethernet port (LAN1) is 192.168.0.1 .

S2: Pressing the reset button: The 3302, 3306, 6602, and 6606 all require that the unit be powered. The user has to wait for an LED to signal that it is time to press and hold the button. The 3305 is different because there is no LED under software control. Refer to the model specific section for each model.

***P*:** How do I regain administrative use of the serial port?
S: The serial port is always active as a configuration port unless it's configured as a TCP or UDP server. To regain the port for configuration, either use the web browser configuration to re-configure the port or use the initial configuration described in this manual.

Checking Bridge Operation

Once the bridge is installed on your Network, you verify proper operation by testing its functionality. Attempt to send packets through it, to verify its operation. The procedure is as follows.

From a PC on one side of the bridge, ping a PC on the other side of the bridge, or attempt a web connection to a web server on the other side of the bridge. If either method succeeds, then two-way operation is confirmed.

If any one PC on one side of the bridge can communicate with any single PC or server on the other side of the bridge, then the bridge configuration is likely correct and other problems should be investigated with a larger view of the network in mind.

You will not be able to ping or contact any devices on the Internet from a PC on the trusted inteface through the bridge. It is normally a "hard firewall" and only transfers packets to the remote bridges.

Remember that this unit is a bridge, not a router. All IP addresses on the trusted side of ALL bridges in the system should be in the same IP subnet address range.

Appendix A

Specifications

XT-6632 Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100/1000BaseTx, Autosense X2
- USB Interface: USB for certificate transfer
- Serial Port (2) RS-232 port for setup or TCP/UDP serial server
- Throughput: Greater than 700 Mbps with AES 256 in UDP mode
- Throughput: Greater than 789 Mbps with AES 256 in TCP mode
- Bridge/Tunnel supports 4096 MAC address table entries
- Power: 120 VAC ~ maximum 75 watts typical
- LED: Over-temperature warning, LAN Activity, LAN status (two per interface), Power
- Default LAN 1 IP address: 192.168.0.1
- Default LAN 2 IP addresses: DHCP Client
- Supports 128 simultaneous client XT, UT, ET, or UT-Soft units
- Browser Management port: 443 (HTTPS)
- Operational Temperature: Office environment
- Dimensions 1U high rack chassis 10.5 x 16.75 x 1.75 Inches plus 19” rack brackets
- Weight 12 pounds

XT-3305 and XT-3305s Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100/1000BaseTx, Autosense
- Contains five “soft” ethernet ports that may be configured as trusted or untrusted
- Sustained throughput: 20 Mbps with AES 256
- Approximately 3500 packets-per-second with 94 byte packets (AES 256).
- Bridge/Tunnel supports 2048 MAC address table entries
- Power: Native 9 to 30 VDC, 12 volt nominal, 5 watts; 120VAC power supply included, -48VDC, 125 VDC, and 240 VAC power supplies available. If POE is used, than a minimum of 24 VDC is recommended and wattage increased to support any attached POE devices.
- LED: LAN Activity, power
- LAN 1 IP address: 192.168.0.1
- LAN 2 IP address: DHCP Client
- LAN 3 IP address: disabled
- RS-232 Serial Port - Rx, Tx, Ground. (XT-3305s only)
- In server mode, supports 8 simultaneous client XT, UT, ET, or UT-Soft units
- Browser Management port: 443 (HTTPS)
- Operational Temperature: -10 to +45C
- Dimensions 110 mm, 4.33” W x 75mm, 2.95” D x 24mm, 0.95” H(including rubber feet)
- Weight 6.17 oz – 175 g

XT-3306 Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100/1000BaseTx, Autosense
- Contains a four port VLAN switch on the trusted interface
- Serial Port: RS-232 port for setup or TCP/UDP serial server
- Sustained throughput: 15 Mbps with AES 256
- Several thousand PPS throughput depending upon packet size
- Bridge/Tunnel supports 2048 MAC address table entries
- Power: Native 8 to 28 VDC, 12 volt nominal, 10 watts; 120VAC power supply included, -48VDC, 125 VDC, and 240 VAC power supplies available
- LED: LAN Activity, LAN status (two per interface), power, status
- Default LAN 1 IP address: 192.168.0.1
- Default LAN 2 IP addresses: DHCP Client
- In server mode, supports 8 simultaneous client XT, UT, ET, or UT-Soft units
- Browser Management port: 443 (HTTPS)
- Operational Temperature: Office environment
- Dimensions 5” x 3.75” x 1”
- Weight one pound

XT-6606 Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100/1000BaseTx, Autosense, one trusted and two untrusted interfaces
- Serial Port: RS-232 port for setup or TCP/UDP serial server
- Sustained throughput: 63 Mbps with AES 256
- Several thousand PPS throughput depending upon packet size
- Bridge/Tunnel supports 2048 MAC address table entries
- Power: Native 12 volt nominal, 6 to 16 watts; 120VAC power supply included, 12 VDC, 24 VDC, -48VDC, 125 VDC, and 240 VAC power supplies available
- LED: LAN Activity, LAN status (two per interface), power
- Default LAN 1 IP address: 192.168.0.1
- Default LAN 2/3 IP addresses: DHCP Client
- In server mode, supports 50 simultaneous client XT, UT, ET, or UT-Soft units
- Browser Management port: 443 (HTTPS)
- Operational Temperature: 0 to +40 C
- Dimensions 6 5/8” x 6 1/4” x 1 1/4”
- Shipping weight: five pounds

XT-3303 Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100/1000BaseTx, Autosense
- Serial Port: RS-232 port for setup or TCP/UDP serial server
- Contains three “soft” Ethernet ports that may be configured as trusted or untrusted
- Sustained throughput: 20 Mbps with AES 256
- Approximately 3500 packets-per-second with 94 byte packets (AES 256).
- Bridge/Tunnel supports 2048 MAC address table entries
- Power: Native 8 to 30 VDC, 12 volt nominal, 5 watts; 120VAC power supply included, -48VDC, 125 VDC, and 240 VAC power supplies available. If passive PoE is used, 11 – 30VDC. A minimum of 18VDC is recommended for long cable runs.
- LED: LAN Activity, power
- LAN 1 IP address: 192.168.0.1
- LAN 2 IP address: DHCP Client
- LAN 3 IP address: disabled
- In server mode, supports 8 simultaneous client XT, UT, ET, or UT-Soft units
- Browser Management port: 443 (HTTPS)
- Operational Temperature: -40 to +70C
- Dimensions: 125 mm, 4.9” W x 215mm, 8.5” D x 39mm, 1.5” H (including rubber feet)
- Weight: 350g, 12.3oz

XT-hEX Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100/1000BaseTx, Autosense
- Contains five “soft” Ethernet ports that may be configured as trusted or untrusted
- Sustained throughput: 20 Mbps with AES 256
- Approximately 3500 packets-per-second with 94 byte packets (AES 256).
- Bridge/Tunnel supports 2048 MAC address table entries
- Power: Native 8 to 30 VDC, 24 volt nominal, 5 watts; 100-240VAC 50/60Hz power supply included, -48VDC, 125 VDC, and 240 VAC power supplies available. If powered via passive POE, 12 VDC minimum, 24VDC recommended.
- LED: LAN Activity, power
- LAN 1 IP address: 192.168.0.1
- LAN 2 IP address: DHCP Client
- LAN 3 IP address: disabled
- In server mode, supports 8 simultaneous client XT, UT, ET, or UT-Soft units
- Browser Management port: 443 (HTTPS)
- Operational Temperature: -40 to +60C
- Dimensions 113 mm, 4.45” W x 89mm, 3.5” D x 30mm, 1.18” H (including rubber feet)
- Weight 248 grams, 10 oz (including power standard power supply)
- USB host port – currently unused.
- SD card slot – currently unused.

XT-6615 Bridge Specifications

- Encryption: AES 128, 192, or 256 bit
- LAN Interfaces: 10/100/1000BaseTx, Autosense, one trusted and three untrusted interfaces
- Serial Port: RS-232 port
- Sustained throughput: 125 Mbps with AES 256 @ packet size 1470
- Sustained packet rate: 11,145 packets-per-second @ packet size 1470
- Bridge/Tunnel supports 4096 MAC address table entries
- Power: 12 VDC, 2.5A, 30 watts.
- Standard power supply adapter: 100-240 VAC 50/60 HZ
- Indicators: LAN Activity, LAN status (two per interface), power, SSD activity
- Default LAN 1 IP address: 192.168.0.1
- Default LAN 2/3/4 IP addresses: DHCP Client
- In server mode, supports 50 simultaneous client XT, UT, ET, or UT-Soft units
- Browser Management port: 443 (HTTPS)
- Operational Temperature: -10 to +50 C
- Humidity: 0 – 95% relative humidity, non-condensing
- Dimensions 4.5” x 4.2” x 1.7”
- Device weight: 1.25 pounds
- Shipping weight: 4 pounds
- Approvals: UL (Power Supply), FCC Part 15 Class B, CE, RoHS
- Export: ECCN 5A002, License exception ENC

Cables

Commonly used cable connections:

Bridge to hub or ethernet switch

Use any commercially available 10/100BaseT cable. If using 100BaseT or 1000BaseT, an appropriately rated cable is required.

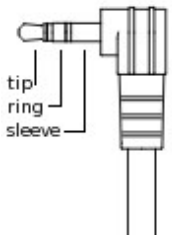
XT-3305s Serial Port

The XT-3305s serial port is implemented using a 2.5mm TRS jack, commonly referred to as a stereo mini-audio jack. The pinning for the jack is shown below.

Tip (T): Rx Data (input to XT-3305s)

Ring(R): Tx Data (output from XT-3305s)

Sleeve(S): Signal ground.



Cables terminated with a TRS plug on one end and a standard DE-9 on the other end are available from DCB.

XT-6615 Serial Port

The XT-6615 serial port is implemented on an RJ45 connector. An adapter is provided to convert from the RJ45 connector to a DE9 female, suitable for direct connection to a PC COM port.

RJ45	DE9	DTE Signal Name	Signal Direction to/from XT-6615
Pin 1	Pin 8	RTS	Output
Pin 2	Pin 6	DTR	Output
Pin 3	Pin 2	TXD	Output
Pin 4	Pin 5	GND	
Pin 5	Pin 5	GND	
Pin 6	Pin 3	RXD	Input
Pin 7	Pin 4	DSR	Input
Pin 8	Pin 7	CTS	Input

The above cable is widely available, often described as a router console management cable.

Appendix B

Open Source Software Information

Some models of the bridge were designed in conjunction with Open Source Linux software.

Introduction

Some models of the bridge were designed and programmed with Open Source Linux software in mind. DCB supports the Open Source software effort and is appreciative of the contribution many open source developers have made to the community

Other open source software used in this product may be obtained from the original developers, and is made available in accordance with GNU licensing terms.

Obtaining the Source Code

For more information on obtaining the source modules for open source code used in this product, send a written request to the following address. Code is provided on CDROM. According to GNU licensing terms, a duplication fee may be charged.

Open Source Software Administrator
Data Comm for Business, Inc.
2949 CR 1000 E
Dewey, IL. 61840